Actiontec®

Wireless

DSL Modem

Model #: GT724WGR

User Manual

Ver 1.1

Solutions for the Digital Life™

Table of Contents

1 Introduction 1
- Minimum System Requirements 1
- Features 2
- Getting to Know the Modem 3

2 Performing a Quick Setup 7
- Accessing Quick Setup Screens 7
- Changing the Password 9

3 Viewing the Modem's Status 11
- Broadband Connection Status 11
- Network Status 14

4 Configuring Wireless Settings 15
- Accessing Wireless Setup 15
- Basic Wireless Setup 17
- Wireless Advanced Settings 17
- Wireless Status 23

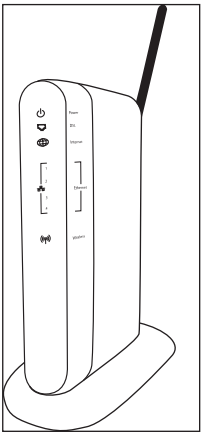
5 Configuring Advanced Setup Options 25
- Accessing the Advanced Setup Options 25
- DSL Settings 27
- DHCP Settings 28
- LAN IP Address 30
- WAN IP Address 31
- QoS Settings Upstream 33
- QoS Settings Downstream 35
- QoS Status 36
- Remote Management 36
- Telnet Timeout Setting 37
- Dynamic Routing 38
- Static Routing 38
- UPnP (Universal Plug and Play) 39
- Time Zone 39
- Remote Syslog Capture 40

6 Configuring Security Settings 41
Accessing Wired Security Screens 41
Admin User Name and Password 42
Firewall 43
Port Forwarding 47
DMZ Hosting 49
NAT (Network Address Translation) 50
7 Configuring Internet Access Controls 51
Accessing Internet Access Control Screens 51
Services Blocking 52
Website Blocking 53
Schedule Rules 54
8 Configuring the Modem's Utilities 57
Accessing the Utilities Screens 57
Restore Default Settings 59
Upgrade Firmware 59
Web Activity Log 60
System Log 61
OAM Ping Test 62
Ping Test 62
Reboot 63
9 Troubleshooting 65
Troubleshooting 65
Frequently Asked Questions 67

A Specifications 73
General 73
Wireless Operating Range 74
LED Indicators 74
Environmental 74
B Setting up Static IPon a Computer 75
Windows 2000 75
Windows XP 80
Windows Vista 83
C Service Acronyms 87
Service Acronym Definitions 87
D Glossary 91
Notices 95
Regulatory Compliance Notices 95
Modifications 95
Limited Warranty 97

Introduction 1

Thank you for purchasing the Actiontec Wireless DSL Modem. The Modem is the simplest way to connect computers to a high-speed broadband connection. This easy-to-use product is perfect for the home office or small business. If you want to take your computing to the next level, the Wireless DSL Modem is sure to be one of the keys to your success.



Minimum System Requirements

- Active DSL service
- Computer with a 10 Mbps or 10/100 Mbps Ethernet connection
- Microsoft Windows 2000, XP, Vista
  Mac OS 7.1+, 8.0+, 9.0+, OS X+
- Internet Explorer 4.0 or higher (5.x+ recommended) or Netscape Navigator 4.0 or higher (4.7+ recommended)
- TCP/IP network protocol installed on each computer

Features

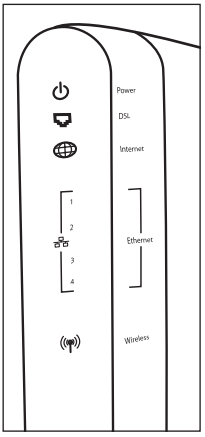
- ADSL WAN port (RJ-11)
- Full-rate ANSI T1.413 Issue 2, ITU G.992.1(G.dmt) and G.992.2(G.lite) standard compliance
- Auto-handshake for different ADSL services
- Bridged Ethernet over ATM, PPP over ATM, PPP over Ethernet
- Precise ATM traffic shaping
- IP packet routing and transparent bridge
- RIP-1, RIP-2, and static routing protocol support
- Built-in NAT, DHCP server
- DNS relay support
- PAP/CHAP authentication, administrative passwords through Telnet
- 64-, 128-, and 256-bit WEP/WPA wireless LAN security
- IEEE 802.3 Ethernet standard compliance
- 10/100 Base-T Ethernet ports (4)
- Fast Ethernet flow control support
- Web-based configuration setup
- FTP firmware upgradeable
- Web download support
- 802.11b/g support

Getting to Know the Modem

This section contains a quick description of the Modem's lights, ports, etc. The Modem has several indicator lights (LEDs) on its front panel and a series of ports on its rear panel.

Front Panel

The front panel of the Modem features eight lights: Power, DSL, Internet, Ethernet (4), and Wireless.



Power Light

The Power light displays the Modem's current status. If the Power light glows steadily green, the Modem is receiving power and fully operational. When the Power light is rapidly flashing, the Modem is initializing. If the Power light glows red when the Power cord is plugged in, the Modem has suffered a critical error and technical support should be contacted.

DSL Light

The DSL light illuminates when the Modem is connected to a DSL line and the unit is able to synchronize to the DSL signal from the ISP. When it flashes, the Modem's built-in DSL modem is training for the DSL service.

Internet Light

When the Internet light glows steadily, the Modem is connected to the DSL provider.

Ethernet Lights

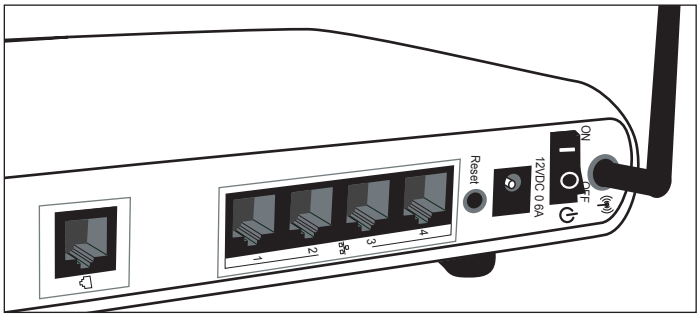
The Ethernet lights illuminate when the Modem is connected to one or more computers via its yellow Ethernet ports.

Wireless Light

The Wireless light illuminates when the Modem's wireless radio is turned on.

Rear Panel

The rear panel of the Modem contains six ports (Ethernet [4], Line, and Power), as well as Reset and Power switches.



Ethernet Ports

The Ethernet ports are used to connect computers to the Modem via Ethernet cable. The Ethernet ports are 10/100 Mbps auto-sensing ports, and either a straight-through or crossover Ethernet cable can be used when connecting to the ports.

Line Port

The Line port is used to connect the Modem to a DSL (Digital Subcriber Line) connection.

Reset Switch

Depressing the Reset switch restores the Modem's factory default settings. To reset the Modem, depress and hold the Reset switch for five to seven seconds. The reset process will start after releasing the switch, during which the Power light will turn from green to orange.

Power Port

The Power port is used to connect the Power cord to the Modem.

Warning: Do not unplug the Power cord from the Modem during the reset process. Doing so may result in permanent damage to the Modem.

Power Switch

The Power switch is used to power the Modem on and off.

This page left intentionally blank.

Performing a Quick Setup

2

This chapter is a guide through a quick set up of the Modem, including how to connect the Modem to the ISP.

To complete the quick setup, have the Welcome Letter or ISP Worksheet handy. If the document is not available, contact the ISP immediately.

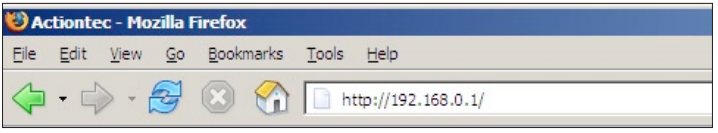
Accessing Quick Setup Screens

To access the Quick Setup screens:

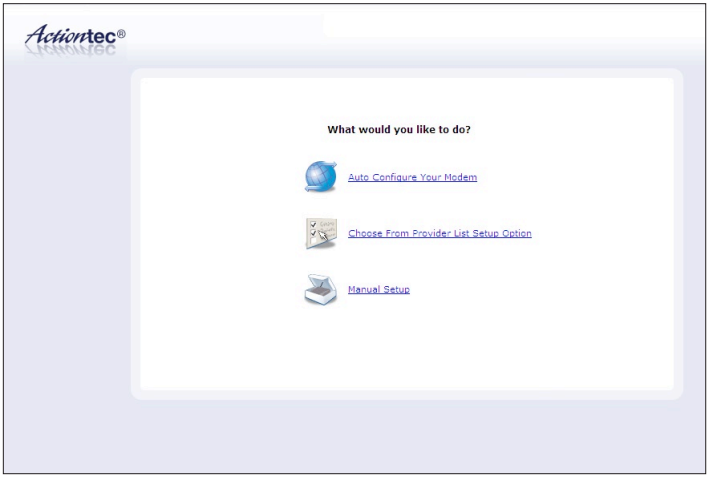
1. Open a Web browser. In the "Address" text box, type:

   `http://192.168.0.1`

   then press **Enter** on the keyboard.



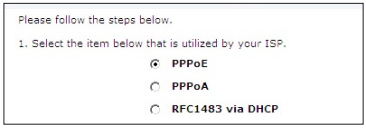
2. Another screen appears. Click **Manual Setup for Internet Access**.



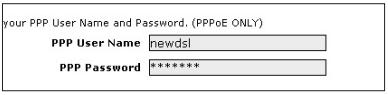
3. Follow the instructions in the "Welcome to the Quick Setup" screen, then click **Next**.

Welcome to the Quick Setup
Before you begin, please make sure you have completed the following steps.
1. The Black or Gray Cable is firmly plugged into your Phone Jack and into the Gray Port on the DSL Gateway.
2. Please make sure that your ISP has provided you with the necessary setup information to configure the Gateway.
Click NEXT to continue.
Next

4. At the top of the next window, select **the type of connection used by the ISP.**

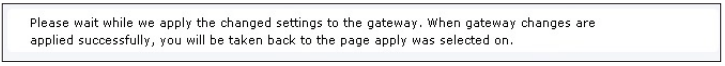


4a. If PPPoA or PPPoE was selected in step 4, the default user name and password are entered in the appropriate text boxes.
If "RFC1483 via DHCP" was selected, go to step 5.



5. Click **Apply** at the bottom of the screen.

6. Read the instructions on the next screen. The Modem is successfully configured.


Please wait while we apply the changed settings to the gateway. When gateway changes are applied successfully, you will be taken back to the page apply was selected on.

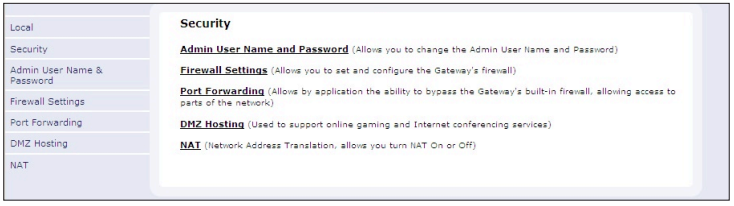
The Power light flashes rapidly while the Modem restarts, then glows steadily green when fully operational. The Internet light will also glow steadily green. The Modem is now configured and users can start surfing the Internet.
If an error appears, stating the Web browser was unable to connect to the Internet, check the configuration settings. Ensure all the information required by the ISP is entered correctly.

Changing the Password

To create or change the password allowing access to the Modem's Web Configuration screens, follow these instructions:

1. From the "Home" screen, select **Security**.

2. The "Security" screen appears. Select "Admin User Name and Password."

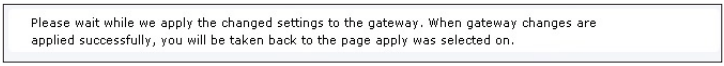

Local
Security
Admin User Name & Password
Firewall Settings
Port Forwarding
DMZ Hosting
NAT
Security
Admin User Name and Password (Allows you to change the Admin User Name and Password)
Firewall Settings (Allows you to set and configure the Gateway's firewall)
Port Forwarding (Allows by application the ability to bypass the Gateway's built-in firewall, allowing access to parts of the network)
DMZ Hosting (Used to support online gaming and Internet conferencing services)
NAT (Network Address Translation, allows you turn NAT On or Off)

3. The "Change Admin Username/Password" screen appears. Enter a new Username in the "Admin User Name" text boxt, then enter a new password in the "Admin Password" text box. Make sure to write down the user name and password and keep it in a secure location. They will be needed to access the Modem's Web Configuration screens in the future.

Local
Quick Setup
Admin User Name & Password
Admin User Name and Password
Enter an admin Username and Password to prevent outsiders from accessing the Gateway's firmware settings. After creating a Username and Password, you will need to enter them everytime you access the Gateway's firmware settings.
Admin User Name:
admin
Admin Password:
Apply

4. Click **Apply** at the bottom of the screen.

5. Read the instructions on the next screen. The user name and password are successfully changed.


Please wait while we apply the changed settings to the gateway. When gateway changes are applied successfully, you will be taken back to the page apply was selected on.

Once the Modem has rebooted, the new user name and password are active. To access the Modem's Web Configuration screens, the new user name and password must be entered.

Viewing the Modem's Status

3

After configuring the Modem, the Modem's connection and network status can be viewed. The Internet connection status is viewed in the "Broadband Connection Status" screen, while the network status is viewed in the "My Network" screen.

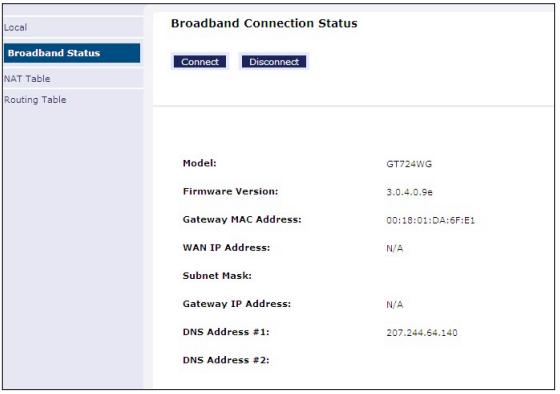
Broadband Connection Status

To view the Modem's connection statistics, select **Status** from the strip of icons at the top of any Gatetway GUI screen. The "Broadband Connection Status" screen appears. There are three sections in this screen: General Statistics, PPP Status, and DSL Status.

☞ ***Note:*** No settings (other than connecting or disconnecting from the Internet by clicking on **Connect** or **Disconnect**) can be changed from the Broadband Connection Status screen.

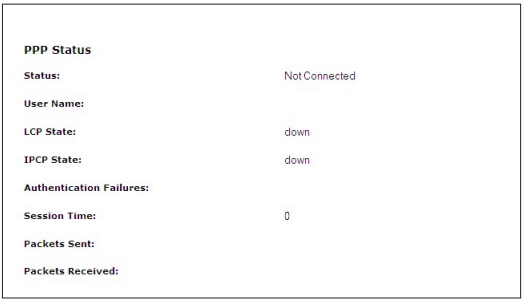
General Statistics

The top section of the Broadband Connection Status screen displays general statistics regarding the Modem, including model number, firmware version, IP address, and gateway IP address.



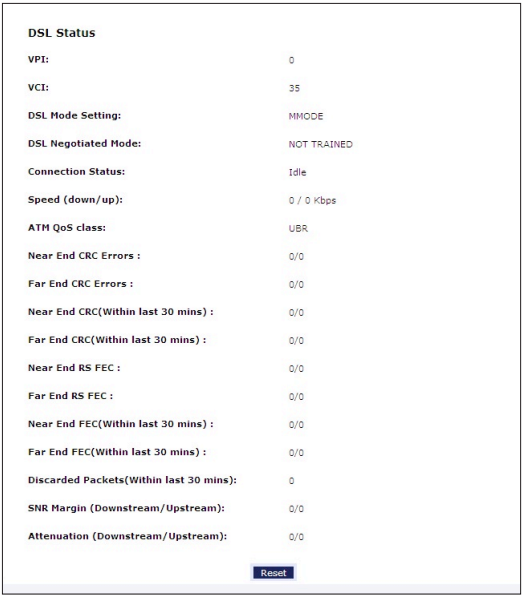
PPP Status

The middle section of the Broadband Connection Status screen displays the status of the Modem's PPP connection, including user name, authentication failures, and packets sent and received.



DSL Status

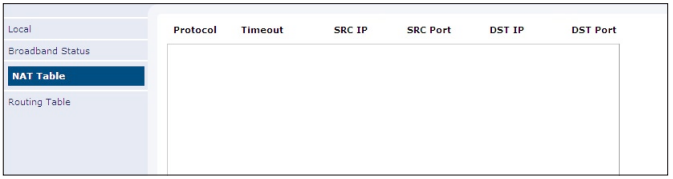
The bottom section of the Broadband Connection Status screen displays the status of the Modem's DSL connection, including mode settings, connection status, and number of discarded packets. Click **Reset** to refresh all statistics on this screen.



In the menu on the left side of the Broadband Connection Status screen, there are two other options available to view: **NAT Table** and **Routing Table**. Click to generate the option of choice.

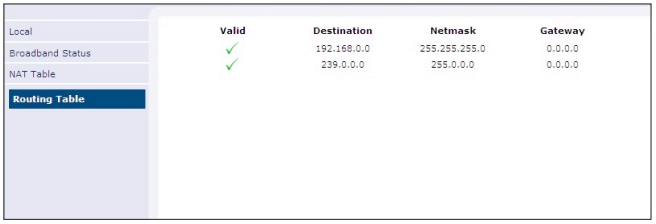
NAT Table

Selecting **NAT Table** generates the "NAT Table" screen. This screen displays an overview of the current list of open connections through NAT (Network Address Translation) the Modem supports between the networked computers and the Internet.



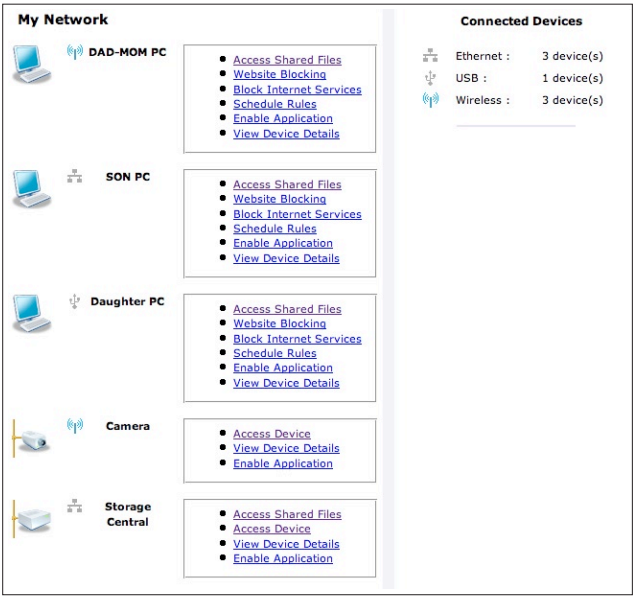
Routing Table

Selecting **Routing Table** generates the "Routing Table" screen. This screen displays an overview of the Modem's network routes.

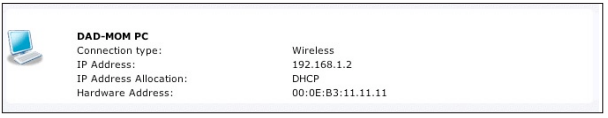


Network Status

To view the Modem's network status, select **My Network** from the strip of icons at the top of any Modem GUI screen. The "My Network" screen appears, listing all devices connected to the network. From this screen, various settings can be accessed, including Website blocking, Schedule Rules, and Enable Application.



To view the network status of a particular device, click **View Device Details** for the device. An overview of the device's network status appears.



Configuring Wireless Settings

4

This chapter explains how to set up the Modem's wireless network capabilities, including setting up wireless security and viewing the wireless connection status.

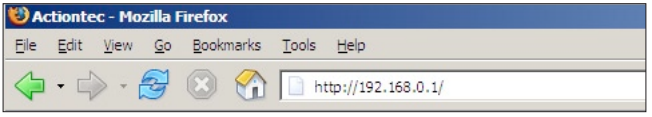
Accessing Wireless Setup

To access the Wireless Settings configuration screens, follow these instructions:

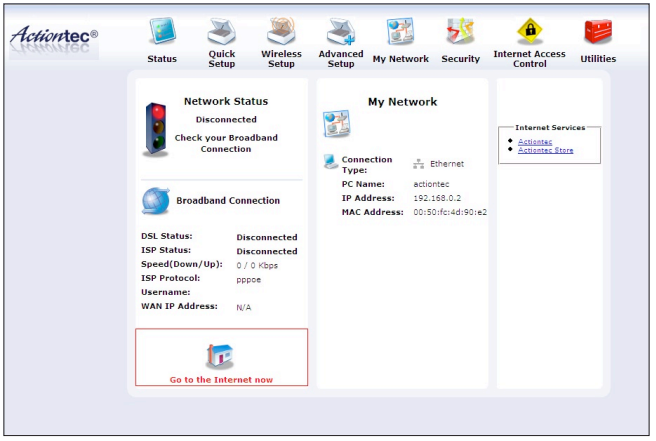
1. Open a Web browser. In the "Address" text box, type:

`http://192.168.0.1`

then press **Enter** on the keyboard.



2. The Main screen appears. Click **Wireless Setup**.

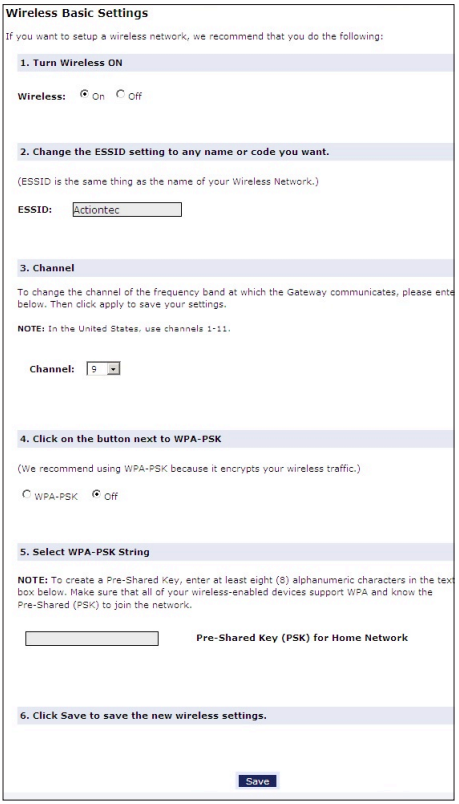


3. A login window appears. Enter the user name and password in the appropriate text boxes, then click **OK**.

Prompt
Enter username and password for "Before configuring the Gateway, a User Name / Password is required. If you do not know the User Name / Password please refer to the User manual for further support." at http://192.168.1.1
User Name:
admin
Password:
****
Use Password Manager to remember this password.
OK
Cancel

☞ ***Note:*** The default user name is "admin." The default password is "password."

4. The "Wireless Basic Settings" screen appears, which guides the user through a basic set up of the Modem's wireless networking capabilities.


Wireless Basic Settings
If you want to setup a wireless network, we recommend that you do the following:
1. Turn Wireless ON
Wireless: On Off
2. Change the ESSID setting to any name or code you want.
(ESSID is the same thing as the name of your Wireless Network.)
ESSID: Actiontec
3. Channel
To change the channel of the frequency band at which the Gateway communicates, please ente
below. Then click apply to save your settings.
NOTE: In the United States, use channels 1-11.
Channel: 9
4. Click on the button next to WPA-PSK
(We recommend using WPA-PSK because it encrypts your wireless traffic.)
WPA-PSK Off
5. Select WPA-PSK String
NOTE: To create a Pre-Shared Key, enter at least eight (8) alphanumeric characters in the tex
box below. Make sure that all of your wireless-enabled devices support WPA and know the
Pre-Shared (PSK) to join the network.
Pre-Shared Key (PSK) for Home Network
6. Click Save to save the new wireless settings.
Save

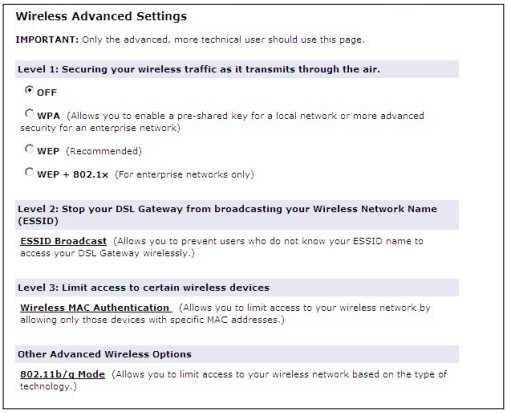
Basic Wireless Setup

To perform a basic setup of a wireless network using the Modem:

1. In the "Wireless Basic Settings" screen, turn the Modem's wireless radio on by selecting **On**.
2. Create a name for the wireless network and enter it in the "ESSID" text box.
3. Select a channel from the "Channel" drop-down menu. In the United States, use channels 1-11.
4. Activate WPA-PSK (Wi-Fi Protected Access w/ Pre-Shared Key) to secure the wireless network by selecting **WPA-PSK**.
5. Enter eight alphamumeric characters in the "Pre-Shared Key (PSK) for Home Network" text box.
6. Click **Save** to save the wireless settings.

Wireless Advanced Settings

To access the Modem's wireless advanced settings screens, select **Advanced Settings** from the menu on the left side of the "Wireless Basic Settings" screen.


Wireless Advanced Settings
IMPORTANT: Only the advanced, more technical user should use this page.
Level 1: Securing your wireless traffic as it transmits through the air.
OFF
WPA (Allows you to enable a pre-shared key for a local network or more advanced security for an enterprise network)
WEP (Recommended)
WEP + 802.1x (For enterprise networks only)
Level 2: Stop your DSL Gateway from broadcasting your Wireless Network Name (ESSID)
ESSID Broadcast (Allows you to prevent users who do not know your ESSID name to access your DSL Gateway wirelessly.)
Level 3: Limit access to certain wireless devices
Wireless MAC Authentication (Allows you to limit access to your wireless network by allowing only those devices with specific MAC addresses.)
Other Advanced Wireless Options
802.11b/g Mode (Allows you to limit access to your wireless network based on the type of technology.)

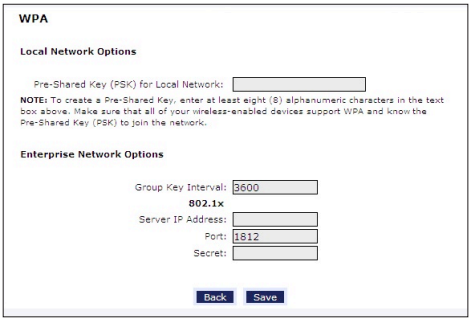
This generates the "Wireless Advanced Settings" screen. In this screen, the security of the wireless network can be activated and fortified.

Wireless Security

The first section of the Wireless Advanced Settings screen involves wireless security (securing wireless traffic as it transmits through the air). The Modem offers three types of wireless security: WPA WEP, and WEP+802.1x..

WPA

Activating **WPA** (Wi-Fi Protected Access) in the Wireless Advanced Settings screen generates the "Wireless WPA Settings" screen.


WPA
Local Network Options
Pre-Shared Key (PSK) for Local Network:
NOTE: To create a Pre-Shared Key, enter at least eight (8) alphanumeric characters in the text box above. Make sure that all of your wireless-enabled devices support WPA and know the Pre-Shared Key (PSK) to join the network.
Enterprise Network Options
Group Key Interval: 3600
802.1x
Server IP Address:
Port: 1812
Secret:
Back
Save

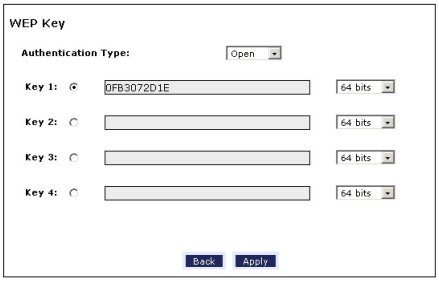
There are two levels of WPA. "Pre-Shared Key (PSK) for Home Network" is for home network security. To set up a PSK (Pre-Shared Key), enter 8-63 alphanumeric characters in the text box. All wireless-enabled devices must support WPA and know the PSK to join the network.

The "Group Key Interval," "Server IP Address," "Port," and "Secret" text boxes are enterprise network specific, and should only be accessed by an information systems professional. See "WEP+802.1x" on the previous page for more information.

When finished with this screen, click **Apply** to save all changes. To return to the Wireless Advanced Settings screen, click **Back**.

WEP

Selecting **WEP** in the Wireless Advanced Settings screen generates the "WEP Key" screen. Here, the authentication type, encryption level, and WEP keys are entered to activate WEP (Wired Equivalent Privacy) security encryption for the wireless network.



Authentication Type - There are three authentication types: Open, Shared, and Both. Open authenticaton allows any wireless-enabled device to recognize the network, even if the WEP key is invalid. Shared allows only wireless-enabled devices with the correct WEP key to recognize the network.

64-bit WEP - 64-bit WEP requires one or more keys, each key comprising five hexadecimal pairs. One key (Key 1) is automatically generated by the Modem at start-up, based on the Modem's MAC address. This key is also displayed on a sticker on the bottom of the Modem. A hexadecimal digit consists of an alphanumeric character ranging from 0-9 or A-F. An example of a 64-bit WEP key is: 4E-A3-3D-68-72. To create a new set of 64-bit WEP keys, activate one or more keys by clicking in the appropriate circles, then enter five hexadecimal digit pairs in each activated **Key** text box (**Key 1-**, **Key 2-**, **Key 3-**, **Key 4-**). After activating 64-bit WEP, a computer with wireless capability can join the network only if these same keys are entered in the computer's wireless encryption scheme.

128-bit WEP - 128-bit WEP requires one or more keys, each key comprising 13 hexadecimal pairs. A hexadecimal digit consists of an alphanumeric character ranging from 0-9 or A-F. An example of a 128-bit WEP key is: 3D-44-FE-6C-A1-EF-2E-D3-C4-21-74-5D-B1. To create a 128-bit WEP key, activate **Key 1** by clicking in the appropriate circle, select "128 bit" from the drop-down list on the right, then enter 13 hexadecimal digit pairs in the **Key** text box. After activating 128-bit , a computer with wireless capability can join the network only if this key is entered in the computer's wireless encryption scheme.

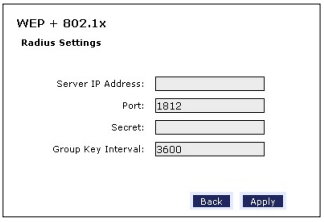
256-bit WEP - 256-bit WEP requires one or more keys, each key comprising 29 hexadecimal pairs. A hexadecimal digit consists of an alphanumeric character ranging from 0-9 or A-F. To create a 256-bit WEP key, activate **Key 1** by clicking in the appropriate circle, select "256 bit" from the drop-down list on the right, then enter 29 hexadecimal digit pairs in the **Key** text box. After activating 256-bit WEP, a computer with wireless capability can join the network only if this key is entered in the computer's wireless encryption scheme.

☞ ***Note***: Not all wireless PC Cards support 128- or 256-bit WEP. Ensure all PC Cards installed in the networked computers support 128- or 256-bit WEP before activating.

When finished with this screen, click **Apply** to save all changes. To return to the Wireless Advanced Settings screen, click **Back**.

WEP+802.1x

Activating **WEP+802.1x** in the Wireless Advanced Settings screen generates the "WEP+802.1x" screen. This setting is for enterprise networks only, and should be accessed by an experienced information systems specialist.



To set up WEP+802.1x security, enter the IP address of the RADIUS server in the "Server IP Address" text box, and the "Secret" key (for communication between the RADIUS server and the Modem) in the "Secret" text box. The "Port" and "Group Key Interval" values should remain the same.

When finished with this screen, click **Apply** to save all changes. To return to the Wireless Advanced Settings screen, click **Back**.

ESSID Broadcast

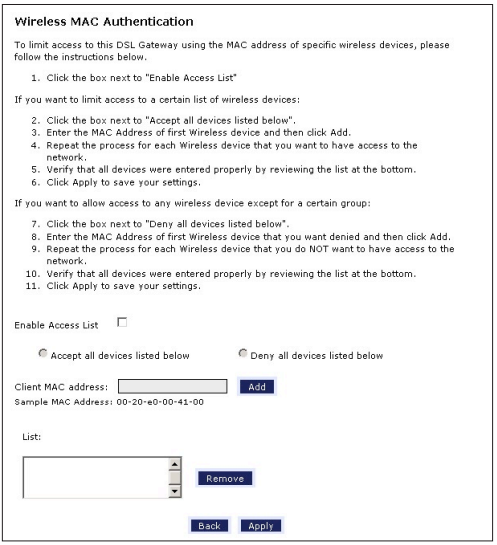
Selecting **ESSID Broadcast** in the Wireless Advanced Settings screen generates the "ESSID Broadcast" screen.

ESSID Broadcast
When ESSID Broadcast is enabled, it means that any computer or wireless device using the ESSID of "Any" can see your DSL Gateway. To prevent this from happening, disable the ESSID broadcast so that only those Wireless devices with your ESSID can access your DSL Gateway.
Enable
Disable
Back
Apply

To prevent unwanted computers from joining the Modem's wireless network by using an ESSID of "Any," select **Disable** in the ESSID Broadcast screen. To broadcast the wireless network's ESSID, select **Enable**.
When finished with this screen, click **Apply** to save all changes. To return to the Wireless Advanced Settings screen, click **Back**.

Wireless MAC Authentication

Selecting **Wireless MAC Authentication** in the Wireless Advanced Settings screen generates the "Wireless MAC Authentication" screen.

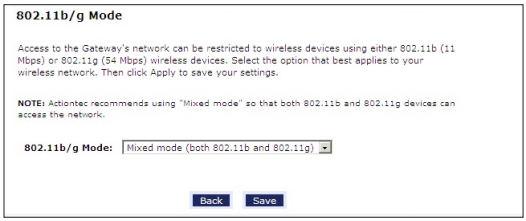

Wireless MAC Authentication
To limit access to this DSL Gateway using the MAC address of specific wireless devices, please follow the instructions below.
1. Click the box next to "Enable Access List"
If you want to limit access to a certain list of wireless devices:
2. Click the box next to "Accept all devices listed below".
3. Enter the MAC Address of first Wireless device and then click Add.
4. Repeat the process for each Wireless device that you want to have access to the network.
5. Verify that all devices were entered properly by reviewing the list at the bottom.
6. Click Apply to save your settings.
If you want to allow access to any wireless device except for a certain group:
7. Click the box next to "Deny all devices listed below".
8. Enter the MAC Address of first Wireless device that you want denied and then click Add.
9. Repeat the process for each Wireless device that you do NOT want to have access to the network.
10. Verify that all devices were entered properly by reviewing the list at the bottom.
11. Click Apply to save your settings.
Enable Access List
Accept all devices listed below
Deny all devices listed below
Client MAC address:
Add
Sample MAC Address: 00-20-e0-00-41-00
List:
Remove
Back
Apply

This feature allows the user to control the wireless LAN network by denying or allowing wireless access by specifying the MAC address of the wireless client(s) allowed or denied access on the wireless network. To do this, follow the instructions on-screen.

When finished with this screen, click **Apply** to save all changes. To return to the Wireless Advanced Settings screen, click **Back**.

802.11b/g Mode

Selecting **802.11b/g Mode** in the Wireless Advanced Settings screen generates the "802.11b/g Mode" screen.


802.11b/g Mode
Access to the Gateway's network can be restricted to wireless devices using either 802.11b (11 Mbps) or 802.11g (54 Mbps) wireless devices. Select the option that best applies to your wireless network. Then click Apply to save your settings.
NOTE: Actiontec recommends using "Mixed mode" so that both 802.11b and 802.11g devices can access the network.
802.11b/g Mode:
Mixed mode (both 802.11b and 802.11g)
Back
Save

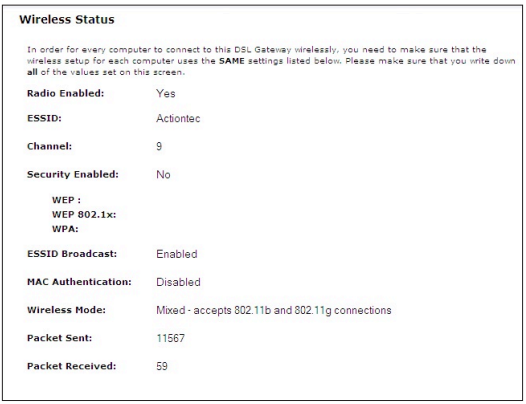
Access to the Modem's network can be restricted to wireless clients using either the 802.11b or 802.11g wireless adapters. Click on the down arrow next to the drop-down menu and select the desired option. We recommend using the "Mixed" mode (the default option), which enables both 802.11b and 802.11g wireless clients to join the network.

☞ ***Note***: If Mixed is chosen and 802.11b wireless clients join the network, some 802.11g wireless clients may connect at 802.11b speeds (11 Mbps) to accomodate the slower adapters.

When finished with this screen, click **Apply** to save all changes.

Wireless Status

To view the Modem's wireless status and settings, select **Wireless Status** from the menu on the left side of the "Wireless Basic Settings" screen.


Wireless Status
In order for every computer to connect to this DSL Gateway wirelessly, you need to make sure that the wireless setup for each computer uses the SAME settings listed below. Please make sure that you write down all of the values set on this screen.
Radio Enabled: Yes
ESSID: Actiontec
Channel: 9
Security Enabled: No
WEP :
WEP 802.1x:
WPA:
ESSID Broadcast: Enabled
MAC Authentication: Disabled
Wireless Mode: Mixed - accepts 802.11b and 802.11g connections
Packet Sent: 11567
Packet Received: 59

The "Wireless Status" screen appears, which displays all of the settings of the Modem's wireless network settings.

This page left intentionally blank.

Configuring Advanced Setup Options

5

This chapter explains how to configure the Modem's advanced setup options, such as Remote Management, DHCP settings, and Quality of Service (QoS).

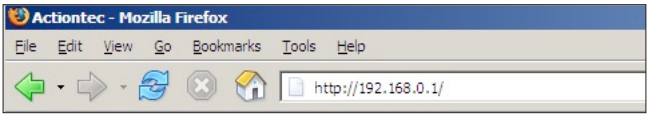
Accessing the Advanced Setup Options

To access the "Advanced Setup" options, follow these instructions:

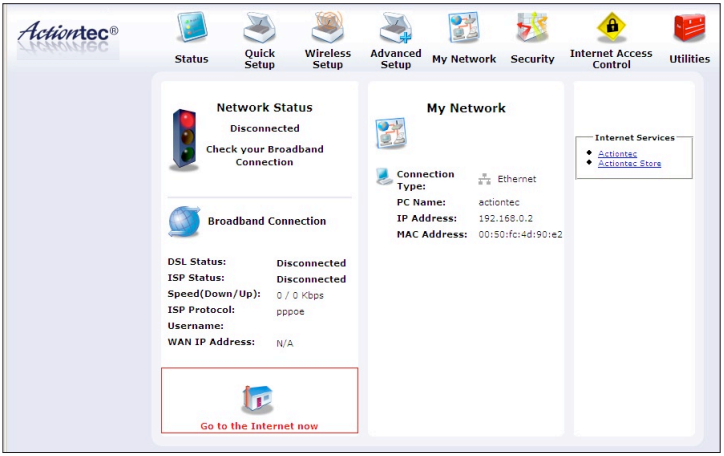
1. Open a Web browser. In the "Address" text box, type:

   `http://192.168.0.1`

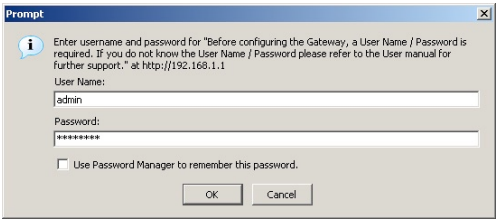
   then press **Enter** on the keyboard.



2. The Main screen appears. Click **Advanced Setup**.

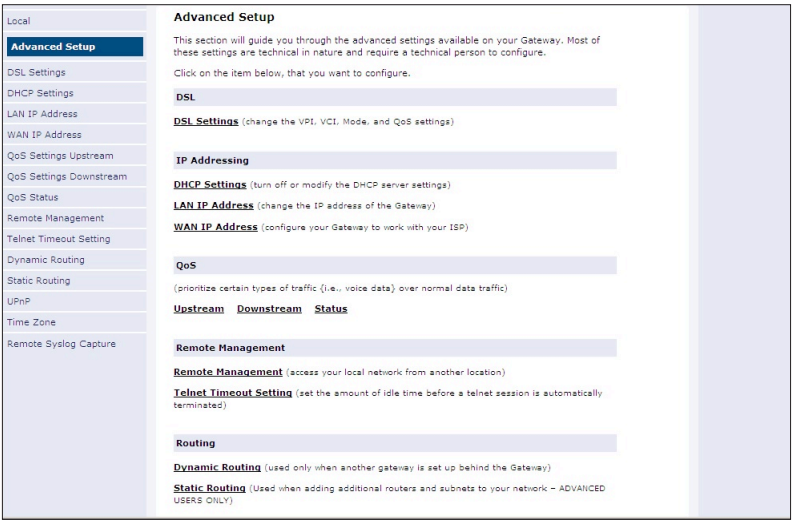


3. A login window appears. Enter the user name and password in the appropriate text boxes, then click **OK**.


Prompt
Enter username and password for "Before configuring the Gateway, a User Name / Password is required. If you do not know the User Name / Password please refer to the User manual for further support." at http://192.168.1.1
User Name:
admin
Password:
****
Use Password Manager to remember this password.
OK
Cancel

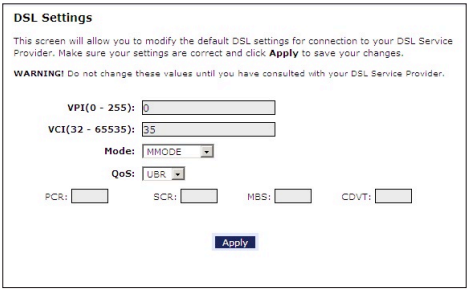
☞ ***Note:*** The default user name is "admin." The default password is "password."

4. The "Advanced Setup" screen appears. To modify a specific configuration, click on its name in the menu bar on the left, or from the list in the middle of the screen.


Local
Advanced Setup
DSL Settings
DHCP Settings
LAN IP Address
WAN IP Address
QoS Settings Upstream
QoS Settings Downstream
QoS Status
Remote Management
Telnet Timeout Setting
Dynamic Routing
Static Routing
UPnP
Time Zone
Remote Syslog Capture
Advanced Setup
This section will guide you through the advanced settings available on your Gateway. Most of these settings are technical in nature and require a technical person to configure.
Click on the item below, that you want to configure.
DSL
DSL Settings (change the VPI, VCI, Mode, and QoS settings)
IP Addressing
DHCP Settings (turn off or modify the DHCP server settings)
LAN IP Address (change the IP address of the Gateway)
WAN IP Address (configure your Gateway to work with your ISP)
QoS
(prioritize certain types of traffic (i.e., voice data) over normal data traffic)
Upstream Downstream Status
Remote Management
Remote Management (access your local network from another location)
Telnet Timeout Setting (set the amount of idle time before a telnet session is automatically terminated)
Routing
Dynamic Routing (used only when another gateway is set up behind the Gateway)
Static Routing (Used when adding additional routers and subnets to your network – ADVANCED USERS ONLY)

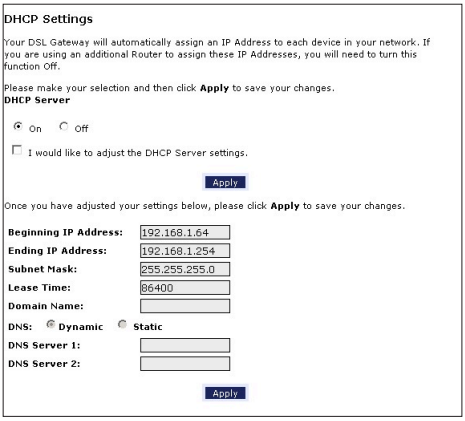
DSL Settings

To access DSL Settings, select **DSL Settings** from the "Advanced Setup" screen. The Modem's VPI, VCI, Mode, and QoS (Quality of Service) settings can be changed from this screen. We recommend not changing these values without first consulting the ISP.


DSL Settings
This screen will allow you to modify the default DSL settings for connection to your DSL Service Provider. Make sure your settings are correct and click Apply to save your changes.
WARNING! Do not change these values until you have consulted with your DSL Service Provider.
VPI(0 - 255): 0
VCI(32 - 65535): 35
Mode: MMODE
QoS: UBR
PCR:
SCR:
MBS:
CDVT:
Apply

DHCP Settings

Selecting **DHCP Settings** in the "Advanced Setup" screen generates the "DHCP Settings" screen. The Modem has a built-in DHCP (Dynamic Host Configuration Protocol) server that automatically assigns a different IP address to each computer on the network, eliminating IP address conflicts.
The factory default setting is **On**. To disable the DHCP Server, select **Off**, then click **Apply**.


DHCP Settings
Your DSL Gateway will automatically assign an IP Address to each device in your network. If you are using an additional Router to assign these IP Addresses, you will need to turn this function Off.
Please make your selection and then click Apply to save your changes.
DHCP Server
On
Off
I would like to adjust the DHCP Server settings.
Apply
Once you have adjusted your settings below, please click Apply to save your changes.
Beginning IP Address: 192.168.1.64
Ending IP Address: 192.168.1.254
Subnet Mask: 255.255.255.0
Lease Time: 86400
Domain Name:
DNS: Dynamic Static
DNS Server 1:
DNS Server 2:
Apply

We strongly recommend leaving the DHCP Server option **On**. If the DHCP Server option is **Off**, ensure the IP addresses of the networked computers are on the same subnet as the IP address of the Modem. For more information, see "DHCP Server Configuration."

DHCP Server Configuration

Clicking in the check box labeled "I would like to adjust the DHCP server settings" activates the text boxes at the bottom of the DHCP Settings screen. Change the IP address range and DNS server information in these text boxes.

Beginning IP Address

This is the IP address at which the DHCP server starts assigning IP addresses. We recommend keeping the factory default setting (192.168.0.2).

Ending IP Address

This is the IP address at which the DHCP server stops assigning IP addresses. We recommend keeping the factory default settings (192.168.0.254).

The beginning and ending IP addresses define the IP address range of the Modem. If the default values are left intact, the Modem supplies a unique IP address between 192.168.0.2 and 192.168.0.254 to each computer on the network. Note that the first three groups of numbers of the addresses are identical; this means they are on the same subnet. The IP address of the Modem must be on the same subnet as the IP address range it generates. For instance, if the Modem's IP address is changed to 10.33.222.1, set the beginning IP address to 10.33.222.2, and the ending IP address to 10.33.222.254.

Subnet Mask

Enter the IP address of the DHCP server's subnet mask here.

Lease Time

This value represents the amount of time (in seconds) the DHCP server holds onto a specific IP address.

Domain Name

This is the domain name provided by the ISP. If the ISP provided domain name information, enter it here. If not, leave the text box intact.

DNS (Dynamic or Static)

This is the type of DNS server provided by the ISP. If ISP provided DNS server information, select the type here. If not, leave as is.

DNS Server 1

This is the primary DNS server provided by the ISP. If the ISP provided DNS server information, enter it here. If not, leave the text box intact.

DNS Server 2

This is the secondary DNS provided by the ISP. If the ISP provided secondary DNS server information, enter it here. If not, leave the text box intact.

When finished in this screen, click **Apply** to activate any changes made.

LAN IP Address

Selecting **LAN IP Address** in the "Advanced Setup" screen causes a warning screen to appear.

LAN IP Address
WARNING!!
Any changes made to the LAN IP Address will reset some of the other settings on the Gateway.
Do not proceed without understanding the technical impacts of changing this feature.
Do you want to proceed?
Yes
No

Read the on-screen warning, then click **Yes** to continue.

The "LAN IP Address" screen appears.

LAN IP Address
Actiontec recommends that you keep the current default LAN IP Address of the DSL Gateway, which is 192.168.0.1.
To make changes, enter the new IP Address or Subnet Mask of the DSL Gateway below.
Modem IP Address:
192.168.0.1
Modem Subnet Mask:
255.255.255.0
Apply

The values in the "Modem IP Address" and "Modem Subnet Mask" text boxes are the IP and subnet mask address of the Modem as seen on the network. These values can be modified for your LAN network, but we recommend keeping the default factory settings (IP address 192.168.0.1; subnet mask address 255.255.255.0).

Note: If the Modem's LAN IP Address is modified, verify that the DHCP Server range is within the same subnet. For more information, see "DHCP Server Configuration."

When finished in this screen, click **Apply** to activate any changes made.

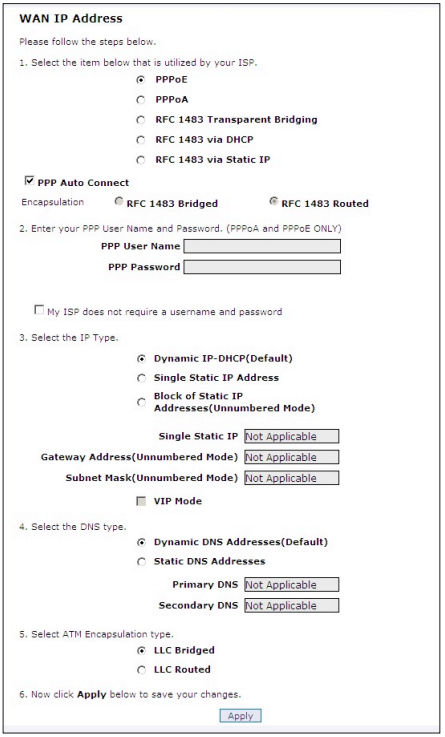
WAN IP Address

Selecting **WAN IP Address** in the "Advanced Setup" screen causes a warning screen to appear.

WAN IP Address
WARNING!!
Any changes made to the WAN IP Address will reset some of the other settings on the Gateway. Do not proceed forward unless you have been instructed to do so by your ISP support personnel.
Do you want to proceed?
Yes
No

Read the on-screen warning, then click **Yes** to continue.

The "WAN IP Address" screen appears.



WAN IP Address allows manual set up of the IP address of the Modem. To do this:

☞ ***Note***: Some DSL providers use PPPoE to establish communication with an end user. Other types of broadband Internet connections (such as fixed point wireless) may use either DHCP or static IP address. If unsure which connection is present, check with the ISP before continuing.

1. Select the type of connection the ISP uses. If PPP Auto Connect is being used, click in the appropriate check box.

2. If using PPPoA or PPPoE was selected in step 1, enter the user name and password in the appropriate text boxes. If the ISP requires no user name or password, click in the "My ISP does not require a username and password" check box.

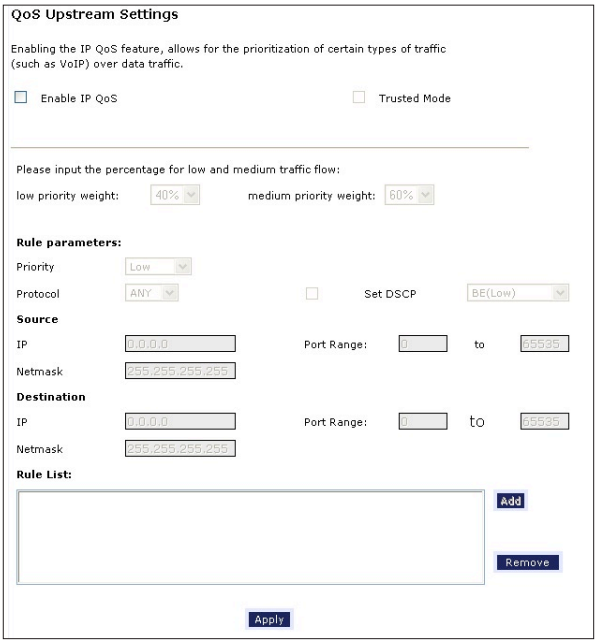
3. Select the IP type. If "Single Static IP Address" was selected, enter the IP address in the "Single Static IP" text box. If "Block of Static IP Addresses" was selected, enter the designated gateway IP address and subnet mask address in the "Modem Address" and "Subnet Mask" text boxes, respectively. Also, "VIP Mode" can be activated by clicking in the appropriate check box.

4. Select the DNS type. If static DNS address was selected, enter the primary DNS address and, optionally, the secondary DNS address in the appropriate text boxes.

When finished in this screen, click **Apply** to activate any changes made.

QoS Settings Upstream

Selecting **QoS Settings Upstream** from the "Advanced Setup" screen causes the "QoS Upstream Settings" screen to appear.



QoS (Quality of Service) allows the prioritization of certain types of data traffic (such as VoIP traffic) over other types of traffic (such as standard data). Both upstream (data coming into the network) and downstream (data going out of the network) traffic can be prioritzed using QoS.

Enable QoS

Clicking in this check box activates/deactivates QoS.

Trusted Mode

If "Trusted Mode" is activated, all data traffic set to an IP precedence level of 5 will be recognized as high priority traffic, regardless of IP or MAC address rule settings (used for VoIP only).

Total Available Bandwidth

Displays the total amount of available bandwidth (in kilobits per second).

High Priority Bandwidth

Enter the amount of high priority bandwidth to be used by the prioritized traffic type (cannot exceed total available bandwidth).

Priority

Always set to "High" and cannot be changed.

Protocol

Select the data type being configured. Options: TCP, UDP, ICMP.

Source

Identify the source device here, using the device's IP or MAC address, then enter appropriate value in text box. If IP is used, enter the netmask address, if applicable. A priority port range can also be defined, using the "Port Range" text boxes.

Destination

Identify the destination device here, using the device's IP address, then enter appropriate value in text box. Enter the netmask address, if applicable. A priority port range can also be defined, using the "Port Range" text boxes.

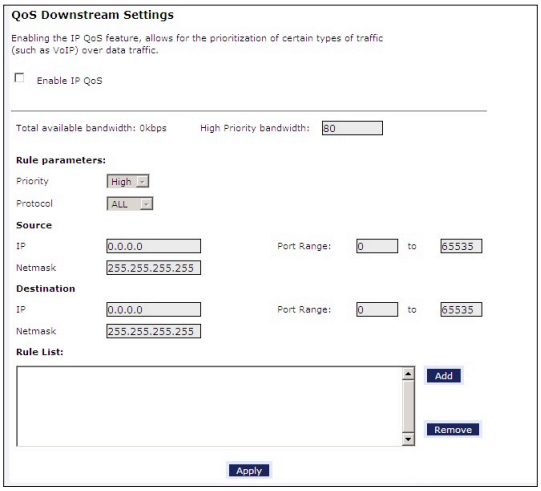
Rule List

After finishing the configuration of the QoS settings, click **Add** to save the settings in the Rule List menu box. This collection of QoS settings can then be reused at a future time. If deleting a QoS rule list, highlight it, then click **Remove**.

When finished, click **Apply** to activate any changes made.

QoS Settings Downstream

Selecting **QoS Settings Downstream** from the "Advanced Setup" screen causes the "QoS Downstream Settings" screen to appear.

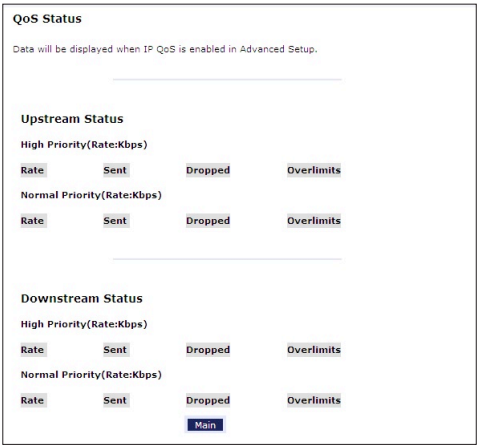


The "QoS Downstream Settings" screen is identical to the "QoS Upstream Settings" screen, with the exception of the "Trusted Mode" and "Set IP Precedence" options. Use this screen to configure QoS for data going out of the network.

When finished in this screen, click **Apply** to activate any changes made.

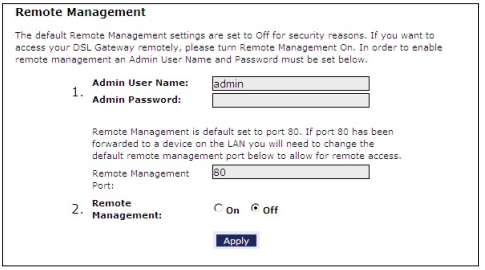
QoS Status

Selecting **QoS Status** from the "Advanced Setup" screen causes the "QoS Status" screen to appear. This screen displays the status of QoS upstream and downstream traffic, and differentiates both streams into high priority and normal priority traffic.



Remote Management

Selecting **Remote Management** in the "Advanced Setup" screen generates the "Remote Management" screen. Remote management allows access to the Modem through the Internet via another computer. The Modem will be vulnerable to other users on the Internet if Remote Management is activated.


Remote Management
The default Remote Management settings are set to Off for security reasons. If you want to access your DSL Gateway remotely, please turn Remote Management On. In order to enable remote management an Admin User Name and Password must be set below.
1.
Admin User Name:
admin
Admin Password:
Remote Management is default set to port 80. If port 80 has been forwarded to a device on the LAN you will need to change the default remote management port below to allow for remote access.
Remote Management Port:
80
2.
Remote Management:
On
Off
Apply

To access the Modem remotely:

1. Enter a user name and password in the appropriate text boxes.

2. Enter a port number through which the Modem will be accessed. Port 80 is the default port number.

3. Activate Remote Management by selecting the appropriate **On** radio button.

4. Write down the WAN IP address of the Modem (see "WAN IP Address").

5. On a computer outside of the network, open a Web browser and enter the Modem's WAN IP address in the Address text box. The Modem's Home screen (or a password prompt, if a password has been set) appears in the browser window.

   Note: If the default port (80) of the Modem has been changed, the user may need to enter the WAN IP, a colon (:), and the new port number. For example, if the WAN IP is 71.251.176.63, and the port has been changed to 8081, enter

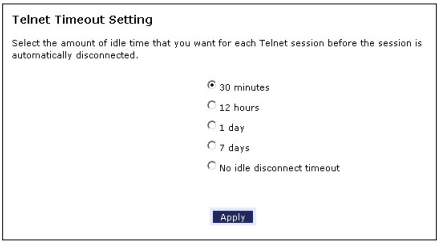
   `http://71.251.176.63:8081`

   to remotely access the Modem.

When finished in this screen, click **Apply** to activate any changes made.

Telnet Timeout Setting

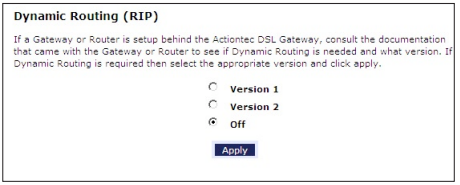
Selecting **Telnet Timeout Setting** in the "Advanced Setup" screen generates the "Telnet Timeout Setting" screen. Select a period of time from the choices available, and the Telnet session will automatically terminate at that time. If no automatic termination is needed, select "No idle disconnect timeout."


Telnet Timeout Setting
Select the amount of idle time that you want for each Telnet session before the session is automatically disconnected.
30 minutes
12 hours
1 day
7 days
No idle disconnect timeout
Apply

When finished in this screen, click **Apply** to activate any changes made.

Dynamic Routing

Selecting **Dynamic Routing** in the "Advanced Setup" screen generates the "Dynamic Routing" screen.

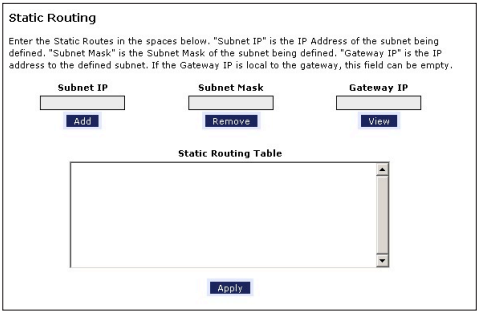

Dynamic Routing (RIP)
If a Gateway or Router is setup behind the Actiontec DSL Gateway, consult the documentation that came with the Gateway or Router to see if Dynamic Routing is needed and what version. If Dynamic Routing is required then select the appropriate version and click apply.
Version 1
Version 2
Off
Apply

If another gateway or router is set up behind the Modem in the network configuration, consult the documentation that came with the other gateway to see what kind of Dynamic Routing is required, then select the needed option.

When finished in this screen, click **Apply** to activate any changes made.

Static Routing

Selecting **Static Routing** in the "Advanced Setup" screen generates the "Static Routing" screen. Enter the static route addresses in their respective text boxes, then click **Add**. The address will appear in the "Static Routing Table." To remove an address, highlight it by clicking on it in the Static Routing Table, then click **Remove**.


Static Routing
Enter the Static Routes in the spaces below. "Subnet IP" is the IP Address of the subnet being defined. "Subnet Mask" is the Subnet Mask of the subnet being defined. "Gateway IP" is the IP address to the defined subnet. If the Gateway IP is local to the gateway, this field can be empty.
Subnet IP
Subnet Mask
Gateway IP
Add
Remove
View
Static Routing Table
Apply

When finished in this screen, click **Apply** to activate any changes made.

UPnP (Universal Plug and Play)

Selecting **UPnP** in the "Advanced Setup" screen generates the "UPnP" screen. In this screen, the Universal Plug and Play option is turned on or off by activating the appropriate circle.

UPnP
Warning: UPnP is disabled by default. If you enable it, it may allow applications to configure the box and allow unexpected traffic to access local devices.
On
Off
Click Apply to continue.
Apply

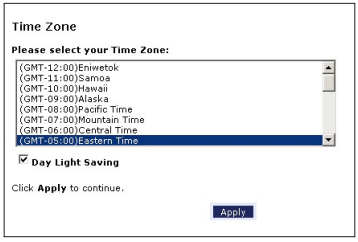
Universal Plug and Play is a zero-configuration networking protocol that allows hardware and software (such as Netmeeting) to operate more efficiently. If Netmeeting is not running properly, activate UPnP.

☞ ***Note***: Activating UPnP presents a slight security risk. After finishing with the hardware or software using UPnP, we recommend deactivating UPnP.

When finished in this screen, click **Apply** to activate any changes made.

Time Zone

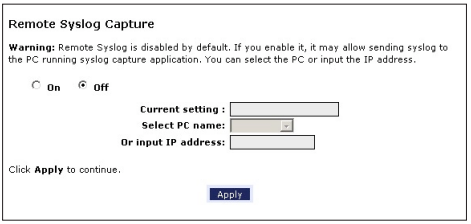
Selecting **Time Zone** in the "Configuring the Advanced Settings" screen generates the "Time Zone" screen. In this screen, select the time zone in which the Modem is being used. Click in the "Day Light Saving" check box if Daylight Saving Time is currently in effect where the Modem is being used.



When finished in this screen, click **Apply** to activate any changes made.

Remote Syslog Capture

Selecting **Remote Syslog Capture** in the "Advanced Setup" screen generates the "Remote Syslog Capture" screen. In this screen, the user can configure the Modem to allow a remote computer to access the Modem's system activity logs.


Remote Syslog Capture
Warning: Remote Syslog is disabled by default. If you enable it, it may allow sending syslog to the PC running syslog capture application. You can select the PC or input the IP address.
On
Off
Current setting :
Select PC name:
Or input IP address:
Click Apply to continue.
Apply

When finished in this screen, click **Apply** to activate any changes made.

Configuring Security Settings

6

This chapter explains how to configure the Modem's wired security capabilities, including firewall settings, DMZ hosting, and network address translation.

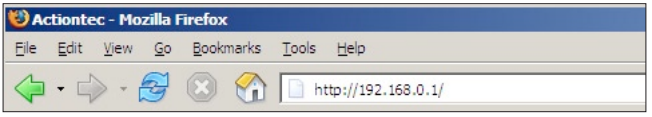
Accessing Wired Security Screens

To access the Wired Security configuration screens, follow these instructions:

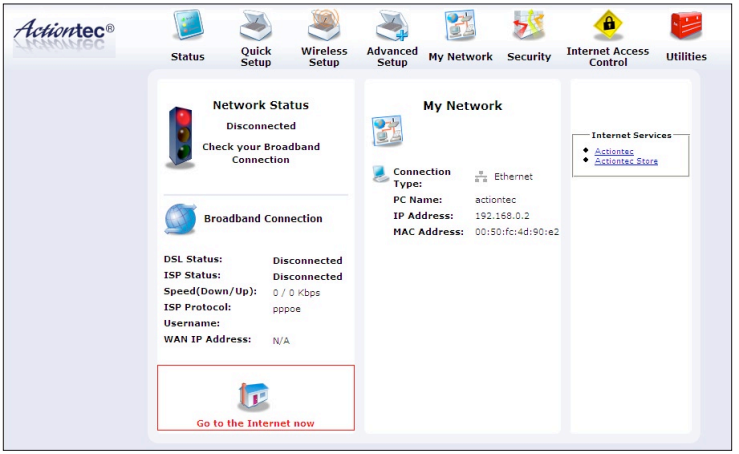
1. Open a Web browser. In the "Address" text box, type:

   `http://192.168.0.1`

   then press **Enter** on the keyboard.



2. The "Home" screen appears. Click **Security**.

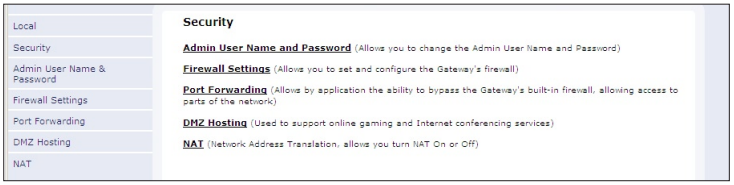


3. A login window appears. Enter the user name and password in the appropriate text boxes, then click **OK**.

Prompt
Enter username and password for "Before configuring the Gateway, a User Name / Password is required. If you do not know the User Name / Password please refer to the User manual for further support." at http://192.168.1.1
User Name:
admin
Password:
****
Use Password Manager to remember this password.
OK
Cancel

☞ ***Note:*** The default user name is "admin." The default password is "password."

4. The "Security" screen appears. To modify a specific configuration, click on its name in the menu bar on the left, or from the list in the middle of the screen.


Local
Security
Admin User Name & Password
Firewall Settings
Port Forwarding
DMZ Hosting
NAT
Security
Admin User Name and Password (Allows you to change the Admin User Name and Password)
Firewall Settings (Allows you to set and configure the Gateway's firewall)
Port Forwarding (Allows by application the ability to bypass the Gateway's built-in firewall, allowing access to parts of the network)
DMZ Hosting (Used to support online gaming and Internet conferencing services)
NAT (Network Address Translation, allows you turn NAT On or Off)

Admin User Name and Password

See "Changing the Password" on page 9.

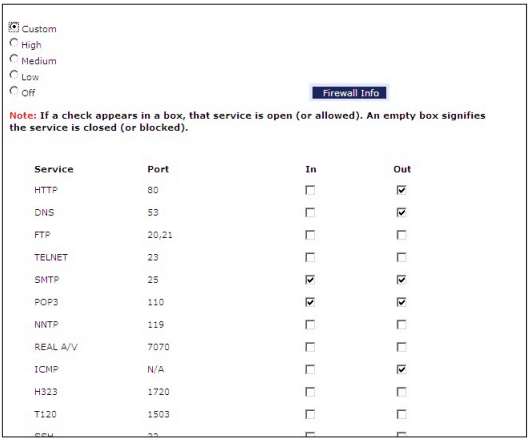
Firewall

Selecting **Firewall** in the Security screen generates the "Firewall Settings" screen. Select the level of security needed for the network.

☞ ***Note***: If VPN connections need to made through the Modem, the Firewall must be set to Off. No VPN connections can be made if the Firewall setting is at Custom, High, Medium, or Low. Also note that DMZ hosting, Port Forwarding, and Application Level Modem settings are active only when the Firewall is Off.

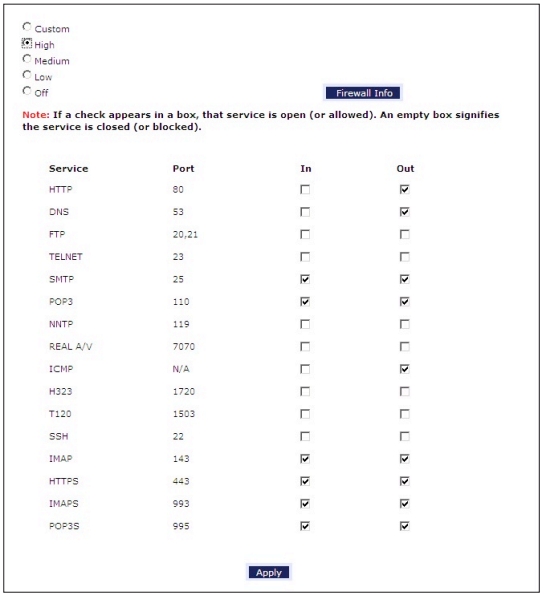
Custom

If **Custom** is selected in the "Firewall Security Level" screen, the user can select which of the services listed in the window can pass through the firewall (both in and outthe services listed at the bottom of the screen. Remember that checking a box opens the service; a blank check box indicates that the service is blocked. Only experienced network administrators should select and use the Custom Firewall option.



High

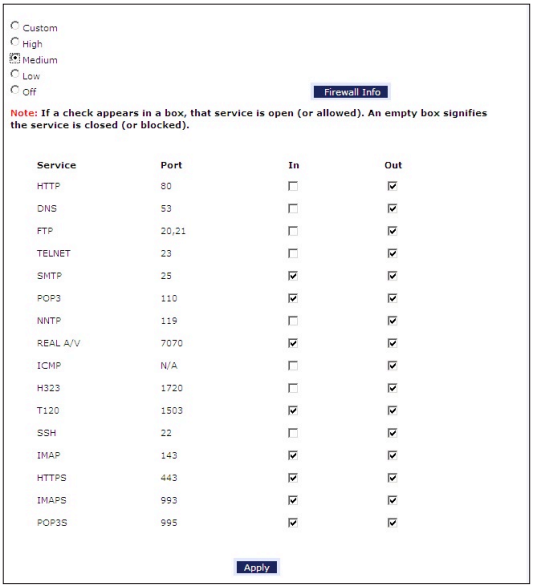
If **High** is selected in the "Firewall Security Level" screen, the services with a check mark beside them will remain open (either incoming, outgoing, or both, depending on the checkmarks), as shown in the figure below. These settings can be modified to customize the firewall settings.



When finished with this screen, click **Apply** to save the changes.

Medium

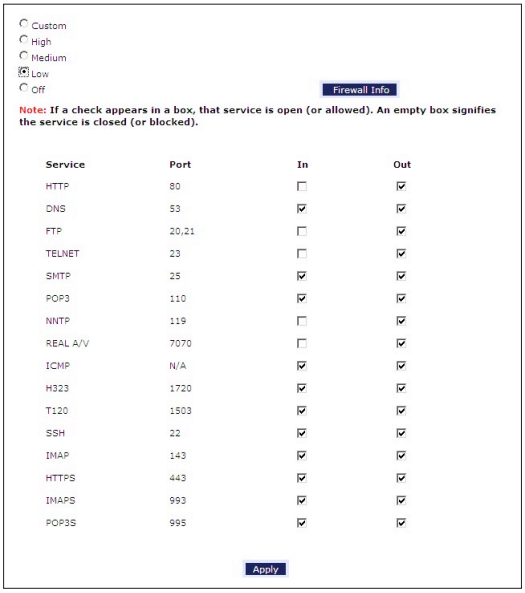
If **Medium** is selected in the "Firewall Security Level" screen, the services with a check mark beside them will remain (either incoming, outgoing, or both, depending on the checkmarks), as shown in the figure below. These settings can be modified to customize the firewall settings.



When finished with this screen, click **Apply** to save the changes.

Low

If **Low** is selected in the "Firewall Security Level" screen, the services with a check mark beside them will remain open (either incoming, outgoing, or both, depending on the checkmarks), as shown in the figure below. These settings can be modified to customize the firewall settings.



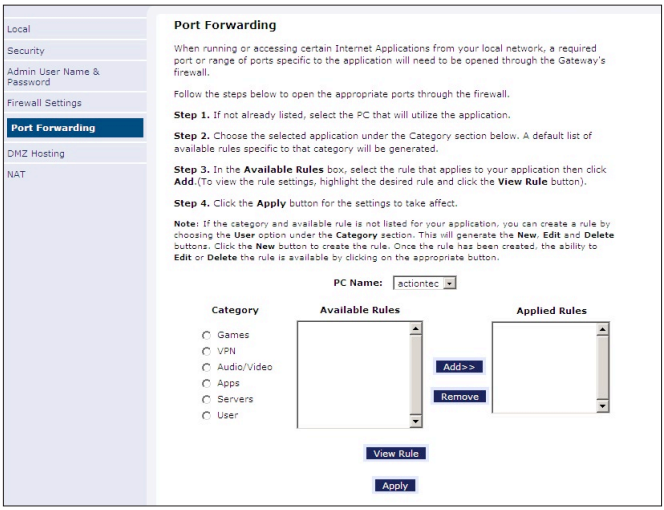
Off

If **Off** is selected in the "Firewall Security Level" screen, firewall filtering is based solely on the basic NAT firewall. At this setting, VPN connections can be made, and DMZ hosting, Port Forwarding, and Applicatiion Level Modem settings are active.

☞ ***Note***: See "Service Acronyms," for a description of the services listed in the Firewall Security Level screens.

Port Forwarding

Selecting **Port Forwarding** in the Security screen generates the "Port Forwarding" screen.


Local
Security
Admin User Name & Password
Firewall Settings
Port Forwarding
DMZ Hosting
NAT
Port Forwarding
When running or accessing certain Internet Applications from your local network, a required port or range of ports specific to the application will need to be opened through the Gateway's firewall.
Follow the steps below to open the appropriate ports through the firewall.
Step 1. If not already listed, select the PC that will utilize the application.
Step 2. Choose the selected application under the Category section below. A default list of available rules specific to that category will be generated.
Step 3. In the Available Rules box, select the rule that applies to your application then click Add.(To view the rule settings, highlight the desired rule and click the View Rule button).
Step 4. Click the Apply button for the settings to take affect.
Note: If the category and available rule is not listed for your application, you can create a rule by choosing the User option under the Category section. This will generate the New, Edit and Delete buttons. Click the New button to create the rule. Once the rule has been created, the ability to Edit or Delete the rule is available by clicking on the appropriate button.
PC Name:
actiontec
Category
Games
VPN
Audio/Video
Apps
Servers
User
Available Rules
Add>>
Remove
Applied Rules
View Rule
Apply

This screen allows certain programs to bypass the Modem's built-in firewall, allowing access to parts of the network (for hosting a Web or ftp server, for example). To use, select the name of a computer on the network from the "PC Name" drop-down list, then click **Add**. Next, select a "Category" by clicking the appropriate radio button. In the "Available Rules" list box, select a game, application, server, etc., then click **Add**>>. The selected item appears in the "Applied Rules" list box. Repeat for each item needed

To remove an item from the Applied Rules list, highlight it, then click **Remove**.

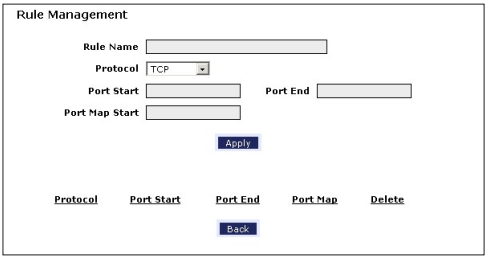
To view an item's rules (forwarded ports, etc.), highlight it, then click **View Rule.**

When finished with this screen, click **Apply** to save the changes.

☞ ***Note***: Port Forwarding is active only when the Firewall is set to Off.

Rule Management

To create a custom set of rules, click the "User" radio button, then click **New**. The "Rule Management" screen appears.



In this screen, the user can create a custom rule not defined in the programming. To do this (using a single port):

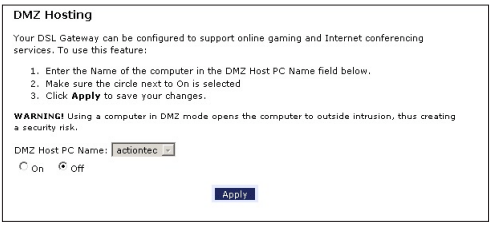
1. Enter the rule name in the "Rule Name" text box. The name is usually based on the application or game title.
2. Set "Protocol" to "TPC."
3. Enter the port number in the "Port Start," "Port End," and "Port Map Start" text boxes. For example, if a server is running on port 8080, enter "8080" in all three text boxes.
4. Click **Apply**.
5. Change Protocol to "UDP."
6. Enter the port number again, as in step 3.
7. Click **Apply** again. The rule's TPC and UDP mapping appear at the bottom of the screen.
8. Click **Back**.
9. Select the computer on which to open the ports, then click **User**.
10. Select the rule, then click **Add** to move the rule to the "Applied Rule" text box.
11. Click **Apply**.

For multiple ports:

1. Enter the rule name in the "Rule Name" text box. The name is usually based on the application or game title.
2. Set "Protocol" to "TPC."
3. Enter the starting port number of the port range in the "Port Start" and "Port Map Start" text boxes, and the last port of the range in the "Port End" text box. For example, if the port range is 5000 to 6000, enter "5000" in the "Port Start" and "Port Map Start" text boxes, and "6000" in the "Port End" text box.
4. Click **Apply**.
5. Change Protocol to "UDP."
6. Enter the port numbers again, as in step 3.
7. Click **Apply** again. The rule's TPC and UDP mapping appear at the bottom of the screen.
8. Click **Back**.
9. Select the computer on which to open the ports, then click **User**.
10. Select the rule, then click **Add** to move the rule to the "Applied Rule" text box.
11. Click **Apply**.

DMZ Hosting

Selecting **DMZ Hosting** in the "Security" screen generates the "DMZ Hosting" screen. To use DMZ hosting, select the computer on the network to be used as a DMZ host in the "DMZ Host PC Name" drop-down menu, then click **On**.

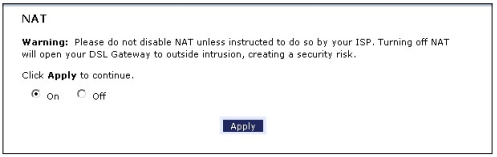

DMZ Hosting
Your DSL Gateway can be configured to support online gaming and Internet conferencing services. To use this feature:
1. Enter the Name of the computer in the DMZ Host PC Name field below.
2. Make sure the circle next to On is selected
3. Click Apply to save your changes.
WARNING! Using a computer in DMZ mode opens the computer to outside intrusion, thus creating a security risk.
DMZ Host PC Name: actiontec
On
Off
Apply

DMZ hosting is used to support online gaming and Internet conferencing services. These programs usually require multiple open ports, making the network accessible from the Internet. DMZ hosting symbolically places the DMZ host computer outside of the Modem's network. We recommend activating DMZ hosting only as long as necessary.
When finished with this screen, click **Apply** to save the changes.

Warning: The DMZ Host computer will be vulnerable to computer hackers on the Internet while in DMZ mode.

NAT (Network Address Translation)

Selecting **NAT** in the "Security" screen generates the "NAT" screen. The Modem's basic firewall security is based on NAT. Disabling NAT allows the computers connected to the Modem to be accessed by outside parties, and can cause the loss of Internet connectivity. Do not turn NAT off unless instructed to do so by the ISP.


NAT
Warning: Please do not disable NAT unless instructed to do so by your ISP. Turning off NAT will open your DSL Gateway to outside intrusion, creating a security risk.
Click Apply to continue.
On
Off
Apply

When finished, click **Apply** to save the changes.

Configuring Internet Access Controls

7

This chapter explains how to configure the Internet access controls of the Modem, such as services blocking, Web site blocking, and schedule rules.

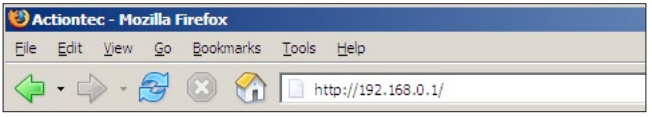
Accessing Internet Access Control Screens

To access the Internet Access Control configuration screens, follow these instructions:

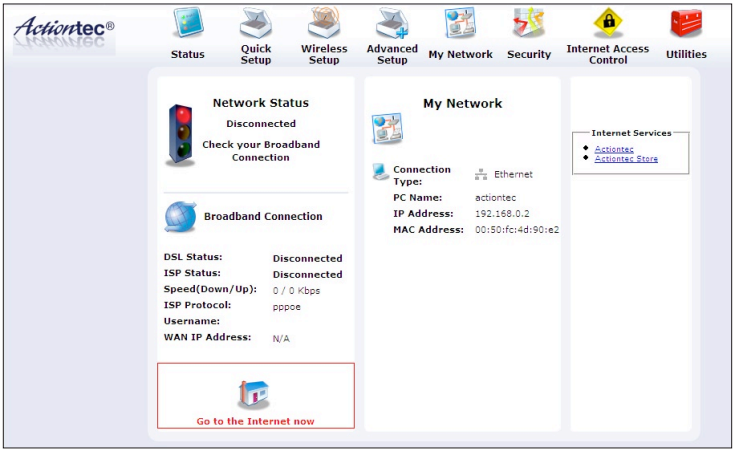
1. Open a Web browser. In the "Address" text box, type:

   http://192.168.0.1

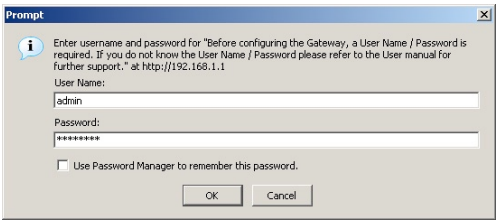
   then press **Enter** on the keyboard.



2. The Main screen appears. Click **Internet Access Control**.



3. A login window appears. Enter the user name and password in the appropriate text boxes, then click **OK**.


Prompt
Enter username and password for "Before configuring the Gateway, a User Name / Password is required. If you do not know the User Name / Password please refer to the User manual for further support." at http://192.168.1.1
User Name:
admin
Password:
****
Use Password Manager to remember this password.
OK
Cancel

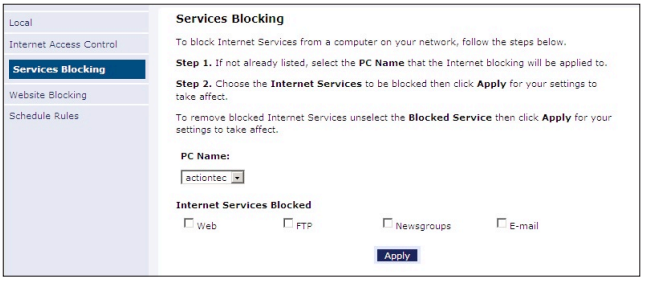
☞ ***Note:*** The default user name is "admin." The default password is "password."

4. The "Internet Access Control" screen appears. To modify a specific setting, click on its name in the menu bar on the left, or from the list in the middle of the screen.

Local
Internet Access Control
Services Blocking
Website Blocking
Schedule Rules
Internet Access Control
Services Blocking (Allows you to block specific Internet services from a specific computer on the network.)
Website Blocking (Allows you to block certain websites from the entire network.)
Schedule Rules (Allows you to set specific scheduling rules for PC on the network.)

Services Blocking

Selecting **Services Blocking** in the Internet Access Control screen generates the "Services Blocking" screen.


Local
Internet Access Control
Services Blocking
Website Blocking
Schedule Rules
Services Blocking
To block Internet Services from a computer on your network, follow the steps below.
Step 1. If not already listed, select the PC Name that the Internet blocking will be applied to.
Step 2. Choose the Internet Services to be blocked then click Apply for your settings to take affect.
To remove blocked Internet Services unselect the Blocked Service then click Apply for your settings to take affect.
PC Name:
actiontec
Internet Services Blocked
Web
FTP
Newsgroups
E-mail
Apply

To modify Internet privileges (Web, FTP, Newsgroups, etc.) for the computers on the network:

1. Select the computer's network name from the "PC Name" drop-down menu.

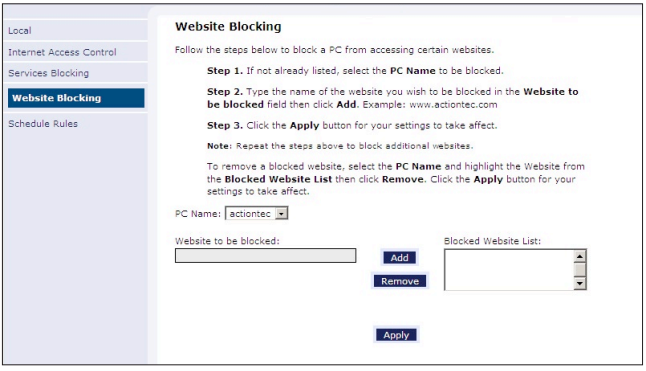
2. Select the Internet service(s) to be blocked by clicking in the appropriate check box.

3. Click **Apply** to block the selected service from the selected computer.

Website Blocking

Selecting **Website Blocking** in the Internet Access Control screen generates the "Website Blocking" screen. This feature enables the Modem to block Web sites to any or all computers on the network. To block a Web site, select the computer name from the "PC Name" drop-down menu. Then, enter the address of the Web site to be blocked in the "Website" text box and click **Add**. The blocked Web site address will be displayed in the "Blocked Website List" text box, and will not be available to the selected computer on the network. To block the Web site from another computer on the network, repeat the process. To remove a blocked Web site, click on it in the "Blocked Website List," then click **Remove**. When finished, click **Apply**.

Any changes made in this screen may take up to five minutes to be applied.


Local
Internet Access Control
Services Blocking
Website Blocking
Schedule Rules
Website Blocking
Follow the steps below to block a PC from accessing certain websites.
Step 1. If not already listed, select the PC Name to be blocked.
Step 2. Type the name of the website you wish to be blocked in the Website to be blocked field then click Add. Example: www.actiontec.com
Step 3. Click the Apply button for your settings to take affect.
Note: Repeat the steps above to block additional websites.
To remove a blocked website, select the PC Name and highlight the Website from the Blocked Website List then click Remove. Click the Apply button for your settings to take affect.
PC Name: actiontec
Website to be blocked:
Add
Remove
Blocked Website List:
Apply

Schedule Rules

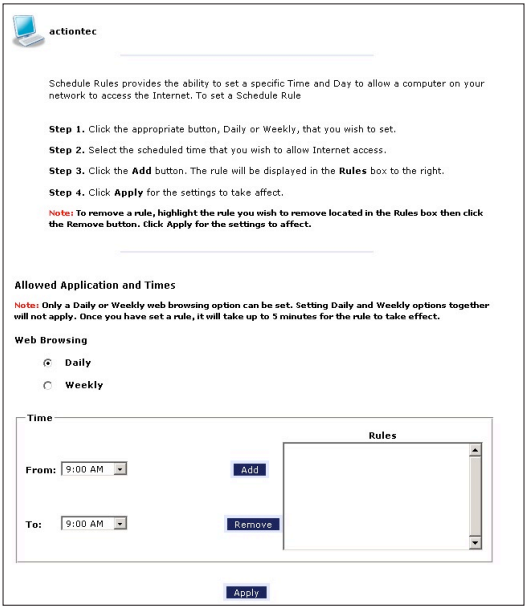
Selecting **Schedule Rules** in the Internet Access Control screen generates the "Schedule Rules" screen. Schedule rules allow computers on the network to access the Internet at scheduled times only.

Local
Internet Access Control
Services Blocking
Website Blocking
Schedule Rules
Schedule Rules
To View the Schedule Rules for a specific PC on your Network, select the PC Name and click the "View/Edit Access Details" link.
PC Name:
actiontec
View/Edit Access Details

To set up schedule rules for a computer on the network:

1. Select the computer's network name from the "PC Name" drop-down menu.

2. Click **View/Edit Access Details**. The computer's "Allowed Application and Times" screen appears.

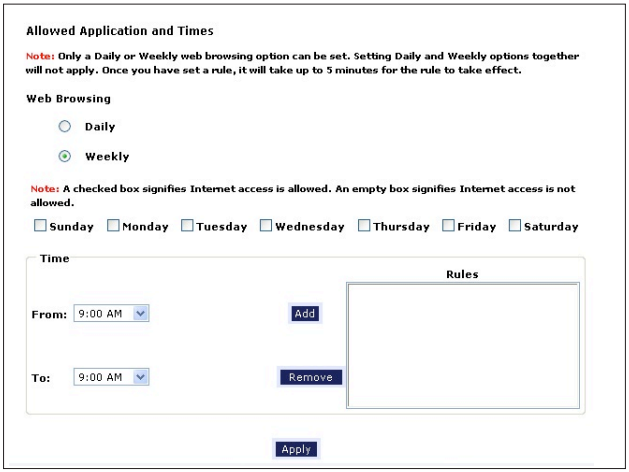

actiontec
Schedule Rules provides the ability to set a specific Time and Day to allow a computer on your network to access the Internet. To set a Schedule Rule
Step 1. Click the appropriate button, Daily or Weekly, that you wish to set.
Step 2. Select the scheduled time that you wish to allow Internet access.
Step 3. Click the Add button. The rule will be displayed in the Rules box to the right.
Step 4. Click Apply for the settings to take affect.
Note: To remove a rule, highlight the rule you wish to remove located in the Rules box then click the Remove button. Click Apply for the settings to affect.
Allowed Application and Times
Note: Only a Daily or Weekly web browsing option can be set. Setting Daily and Weekly options together will not apply. Once you have set a rule, it will take up to 5 minutes for the rule to take effect.
Web Browsing
Daily
Weekly
Time
Rules
From:
9:00 AM
Add
To:
9:00 AM
Remove
Apply

3. To schedule Internet access at the same time every day, select "Daily" by clicking the appropriate radio button. If creating different access schedules on a day-to-day basis, select "Weekly."

4a. If "Daily" was selected in step 3, create a period of Internet access (or rule) by selecting a beginning time (from the "From" drop-down menu) and ending time (from the "To" drop down menu). If allowing Internet access to a particular computer from 6 p.m. to 8 p.m., for example, select "18 (6 pm)" from the From drop-down menu, and "20 (8 pm)" from the To drop-down menu. Click **Add** to add the access period to the "Rules" list box. Additional access periods can be added by repeating this step (9 a.m. through 12 p.m., for example), and adding it to the Rules list box. Once the rules are applied in the Daily screen, Internet access will be granted every day at the times listed in the Rules list box.

☞ ***Note:*** When using "Daily" scheduling, an access period cannot include 12 a.m (midnight). To create an access period that includes midnight, create two access periods, one that ends at 12 a.m., and one that begins at 12 a.m.

4b. If "Weekly" was selected in step 3, periods of Internet access can be scheduled at different times on different days (6 p.m. to 8 p.m. on Friday, and 1 p.m. to 4 p.m. on Saturday, for example). To do this, select the day of the week by clicking in the appropriate check box, then create a access period (or rule), as explained in step 4a. Click **Add** for each separate time period. All access periods created will appear in the Rules list box. Once the rules are applied in the Weekly screen, Internet access will be granted to a particular computer at the days and times selected on a weekly basis.


Allowed Application and Times
Note: Only a Daily or Weekly web browsing option can be set. Setting Daily and Weekly options together will not apply. Once you have set a rule, it will take up to 5 minutes for the rule to take effect.
Web Browsing
Daily
Weekly
Note: A checked box signifies Internet access is allowed. An empty box signifies Internet access is not allowed.
Sunday Monday Tuesday Wednesday Thursday Friday Saturday
Time
Rules
From: 9:00 AM
To: 9:00 AM
Add
Remove
Apply

☞ ***Note:*** When using "Weekly" scheduling, an access period cannot include 12 a.m (midnight). To create an access period that includes midnight, create two access periods, one that ends at 12 a.m. on one day, and one that begins at 12 a.m on the following day.

5. When finished with all scheduling, click **Apply** to save the changes to the Modem.

Removing a Schedule Rule

To remove a scheduled rule, select it from the Rules list box, then click **Remove**. The schedule rule will disappear from the Rules list box.

Configuring the Modem's Utilities

8

This chapter explains how to use the Modem's utilities, including how to restore default settings, upgrade the Modem's firmware, and perform a ping test.

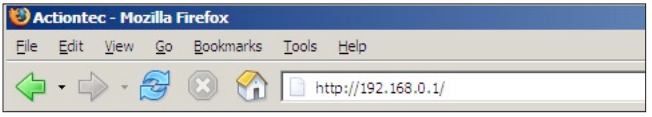
Accessing the Utilities Screens

To access the Utilities configuration screens, follow these instructions:

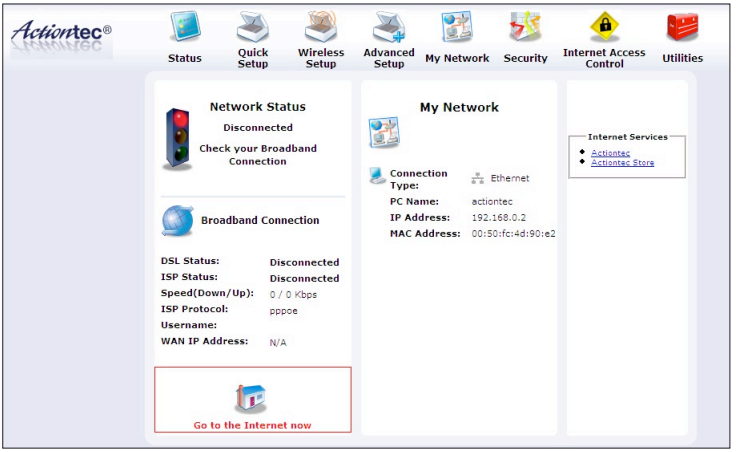
1. Open a Web browser. In the "Address" text box, type:

   `http://192.168.0.1`

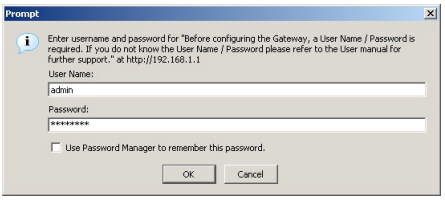
   then press **Enter** on the keyboard.



2. The "Home" screen appears. Click **Utilities**.

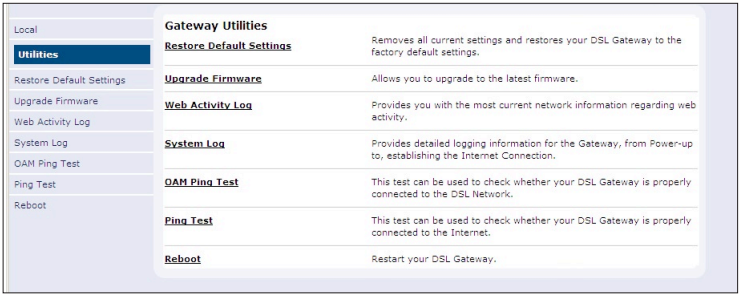


3. A login window appears. Enter the user name and password in the appropriate text boxes, then click **OK**.


Prompt
Enter username and password for "Before configuring the Gateway, a User Name / Password is required. If you do not know the User Name / Password please refer to the User manual for further support." at http://192.168.1.1
User Name:
admin
Password:
****
Use Password Manager to remember this password.
OK
Cancel

☞ ***Note:*** The default user name is "admin." The default password is "password."

4. The "Utilities" screen appears. To modify a specific configuration, click on its name in the menu bar on the left, or from the list in the middle of the screen.


Local
Utilities
Restore Default Settings
Upgrade Firmware
Web Activity Log
System Log
OAM Ping Test
Ping Test
Reboot
Gateway Utilities
Restore Default Settings
Removes all current settings and restores your DSL Gateway to the factory default settings.
Upgrade Firmware
Allows you to upgrade to the latest firmware.
Web Activity Log
Provides you with the most current network information regarding web activity.
System Log
Provides detailed logging information for the Gateway, from Power-up to, establishing the Internet Connection.
OAM Ping Test
This test can be used to check whether your DSL Gateway is properly connected to the DSL Network.
Ping Test
This test can be used to check whether your DSL Gateway is properly connected to the Internet.
Reboot
Restart your DSL Gateway.

Restore Default Settings

To restore the Modem to its factory default settings, select **Restore Default Settings** from the Utilities screen. When the "Restore Default Settings" screen appears, click **Restore Default Settings**. Any changes made to the Modem's settings will be lost and the factory default settings restored. During this process, the Modem's Power light flashes and the Modem is disabled.

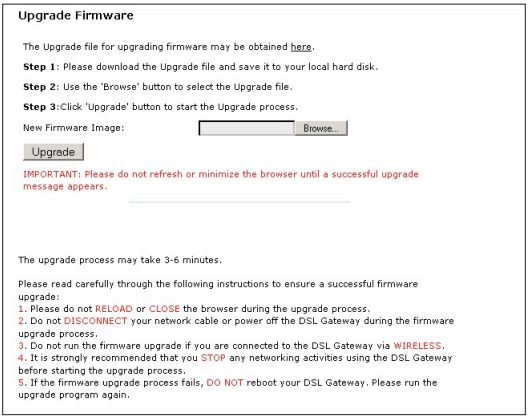
Warning: Do not unplug the Power cord from the Modem during the Restore Default Settings process. Doing so may result in permanent damage to the Modem.

When the Power Light stops flashing and glows steadily green, the Modem is fully operational.

Restore Default Settings
To restore the DSL Gateway to default settings click on the "Restore Default Settings" button below.
Restore Default Settings

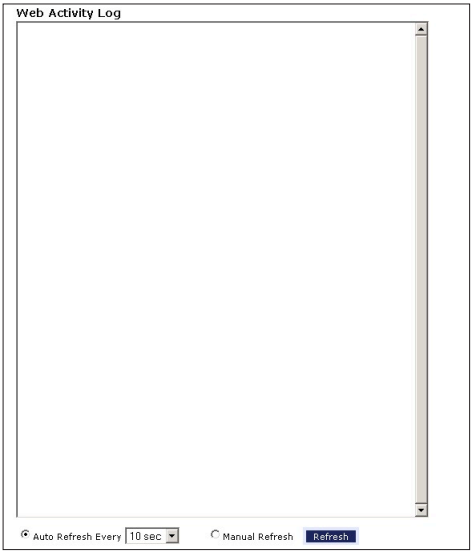
Upgrade Firmware

Selecting **Upgrade Firmware** in the Utilities screen generates the "Upgrade Firmware" screen. Firmware upgrades are periodically released to enhance the Modem's capabilities. Follow the instructions on-screen to upgrade the Modem's firmware.


Upgrade Firmware
The Upgrade file for upgrading firmware may be obtained here.
Step 1: Please download the Upgrade file and save it to your local hard disk.
Step 2: Use the 'Browse' button to select the Upgrade file.
Step 3:Click 'Upgrade' button to start the Upgrade process.
New Firmware Image:
Browse...
Upgrade
IMPORTANT: Please do not refresh or minimize the browser until a successful upgrade message appears.
The upgrade process may take 3-6 minutes.
Please read carefully through the following instructions to ensure a successful firmware upgrade:
1. Please do not RELOAD or CLOSE the browser during the upgrade process.
2. Do not DISCONNECT your network cable or power off the DSL Gateway during the firmware upgrade process.
3. Do not run the firmware upgrade if you are connected to the DSL Gateway via WIRELESS.
4. It is strongly recommended that you STOP any networking activities using the DSL Gateway before starting the upgrade process.
5. If the firmware upgrade process fails, DO NOT reboot your DSL Gateway. Please run the upgrade program again.

Web Activity Log

The Web Activity Log provides information about the Web sites each computer on the Modem's network has visited. To access the Web Activity Log, select **Web Activity Log** from the Utilities screen.



Auto Refresh

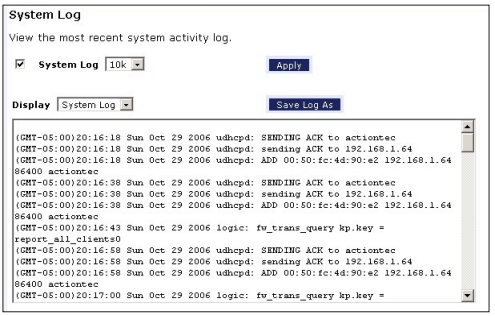
To set the Web Activity Log screen to automatically refresh at certain intervals, activate the circle next to "Auto Refresh Every" at the bottom of the Web Activity Log screen, then enter a time value (in seconds) in the text box, or click on the down arrow and select a time value from the menu that appears. The Web Activity Log will refresh at the selected interval.

Manual Refresh

To set the Web Activity Log screen to manually refresh, activate the circle next to "Manual Refresh" at the bottom of the Web Activity Log screen. To refresh the Web Activity Log screen, click **Refresh**.

System Log

The System Log provides information about the Modem's activity. To access the System Log, select **System Log** from the Utilities screen.


System Log
View the most recent system activity log.
System Log
10k
Apply
Display
System Log
Save Log As
(GMT-05:00)20:16:18 Sun Oct 29 2006 udhcpd: SENDING ACK to actiontec
(GMT-05:00)20:16:18 Sun Oct 29 2006 udhcpd: sending ACK to 192.168.1.64
(GMT-05:00)20:16:18 Sun Oct 29 2006 udhcpd: ADD 00:50:fc:4d:90:e2 192.168.1.64
86400 actiontec
(GMT-05:00)20:16:38 Sun Oct 29 2006 udhcpd: SENDING ACK to actiontec
(GMT-05:00)20:16:38 Sun Oct 29 2006 udhcpd: sending ACK to 192.168.1.64
(GMT-05:00)20:16:38 Sun Oct 29 2006 udhcpd: ADD 00:50:fc:4d:90:e2 192.168.1.64
86400 actiontec
(GMT-05:00)20:16:43 Sun Oct 29 2006 logic: fw_trans_query kp.key =
report_all_clients0
(GMT-05:00)20:16:58 Sun Oct 29 2006 udhcpd: SENDING ACK to actiontec
(GMT-05:00)20:16:58 Sun Oct 29 2006 udhcpd: sending ACK to 192.168.1.64
(GMT-05:00)20:16:58 Sun Oct 29 2006 udhcpd: ADD 00:50:fc:4d:90:e2 192.168.1.64
86400 actiontec
(GMT-05:00)20:17:00 Sun Oct 29 2006 logic: fw_trans_query kp.key =

System Log (Size)

Select the size of the system log displayed here. The smaller the size, the shorter the length of the system log saved.

Display

View other saved logs by selecting a log from this drop-down list.

Apply

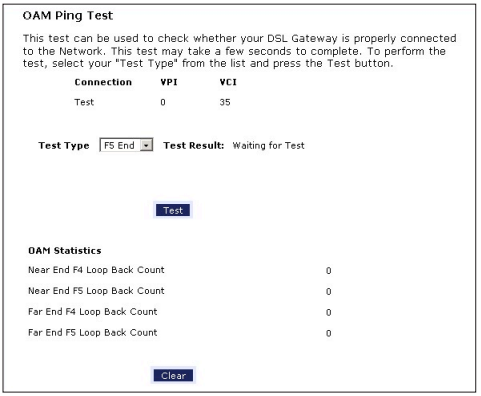
Pressing this button saves any changes to the System Log screen and causes the Save and Restart screen to appear.

Save Log As

Pressing this button allows the user to save a log as a file.

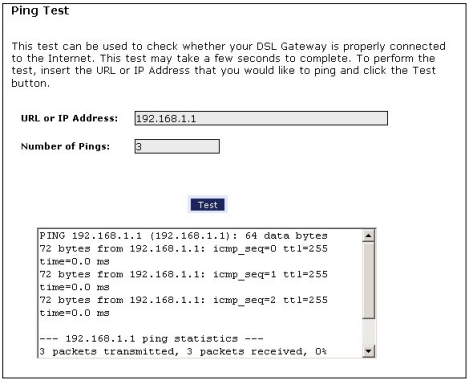
OAM Ping Test

Selecting **OAM Ping Test** from the Utilities screen generates the "OAM Ping Test" screen, which is used to check whether the Modem is properly connected to the network. Follow the on-screen instructions to perform the test.


OAM Ping Test
This test can be used to check whether your DSL Gateway is properly connected to the Network. This test may take a few seconds to complete. To perform the test, select your "Test Type" from the list and press the Test button.
Connection
VPI
VCI
Test
0
35
Test Type
F5 End
Test Result:
Waiting for Test
Test
OAM Statistics
Near End F4 Loop Back Count
0
Near End F5 Loop Back Count
0
Far End F4 Loop Back Count
0
Far End F5 Loop Back Count
0
Clear

Ping Test

Selecting **Ping Test** from the Utilities screen generates the "Ping Test" screen, which is used to check whether the Modem is properly connected to the Internet. Follow the on-screen instructions to perform the test.


Ping Test
This test can be used to check whether your DSL Gateway is properly connected to the Internet. This test may take a few seconds to complete. To perform the test, insert the URL or IP Address that you would like to ping and click the Test button.
URL or IP Address:
192.168.1.1
Number of Pings:
3
Test
PING 192.168.1.1 (192.168.1.1): 64 data bytes
72 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.0 ms
72 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.0 ms
72 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.0 ms
--- 192.168.1.1 ping statistics ---
3 packets transmitted, 3 packets received, 0%

Reboot

Selecting **Reboot** from the Utilities screen generates the "Reboot" screen. From this screen, the Modem can be rebooted. To do this:

1. From the first Reboot screen, click **Reboot**.

2. A confirmation window appears. Click **OK**.

3. The Modem reboots. Read the onscreen information in the screen that appears.

When the Modem's Power light stops flashing, the Modem has rebooted.

This page left intentionally blank.

Troubleshooting 9

This chapter contains a list of problems that may be encountered while using the Modem, and techniques to try and overcome the problem. Note that these techniques may not solve the problem. This chapter also includes a list of frequently asked questions.

Troubleshooting

LAN Connection Failure

- Ensure the Modem is properly configured, the LAN connections are correct, and the power is on.
- Confirm the computer and Modem are on the same network segment. If unsure, let the computer get the IP address automatically by initiating the DHCP function (see "DHCP Server" in chapter 3), then verify the computer is using an IP address within the default range (192.168.0.2 through 198.168.0.254). If the computer is not using an IP address within the range, it will not connect to the Modem.
- Ensure the Subnet Mask address is set to 255.255.255.0 by clicking **Status** in the "Main Menu" screen.

Cannot Connect to the Internet

- Make sure the phone line is connected to the Line port of the modem and the DSL light glows solid green.
- Make sure the Internet light glows solid green.
- If the DSL lightis blinking, contact TDS for a line test, as DSL connectivity has been lost.
- If the Internet light glows red, try power cycling the unit (turning it off, then on). A red Internet light indicates the rejection of username\password by the ISP.
- Ensure both ends of the power cord and all network cables are properly connected.

- Ensure the Subnet Mask address is set to 255.255.255.0 by clicking **Status** in the "Main Menu" screen.

- Verify the Modem's settings are the same as the computer by clicking **Status** in the "Main Menu" screen.

- If running Windows 2000, or XP, check the computer's TCP/IP settings. Select **Start**, **Run**, enter

  CMD

  in the "Open" text box, then press **OK**. A "DOS" window appears, with a blinking cursor (prompt). Enter

  ipconfig

  at the cursor, then press **Enter** on the keyboard.
  The IP address of the Ethernet adapter should appear in the DOS window. Ensure the IP address in the 192.168.0.x network (with "x" defining a range from 2 though 255).
  If the Ethernet adapter is showing an incorrect IP address, enter

  ipconfig /release

  at the cursor, then press **Enter** on the keyboard, which sets all values back to 0 (zero). Next, enter

  ipconfig /renew

  at the cursor, then press **Enter** on the keyboard (this process may take a few seconds). The renewed IP address should be on the 192.168.0.x network.
  If an error occurs, or the IP address renews with an address outside the 192.168.0.x network, contact the ISP immediately

- Ensure the browser is set to "Never dial a connection" and there are no previous LAN settings.
  To check this, go to **Start**, **Settings**, **Control Panel**. In the Control Panel, double-click **Internet Options**. When the "Internet Properties" window appears, ensure that the "Never dial a connection" option is activated, then click **LAN Settings**. When the "Local Area Network (LAN) Settings" window appears, ensure that no settings are activated. If there are settings activated, deactivate them.

- Shutdown and restart the computer. After the computer restarts, unplug the power cord from the Modem and plug it back in. When the lights glow solid green, try accessing the Internet.

Time out error occurs when entering a URL or IP Address

- Verify all the computers are working properly.
- Ensure the IP settings are correct.
- Ensure the Modem is on and connected properly.
- Verify the Modem's settings are the same as the computer by clicking **Status** in the "Main Menu" screen.
- Check the cable/DSL modem by attempting to connect to the Internet.

Frequently Asked Questions

This section includes a list of questions concerning the Modem, and answers to those questions.

General

I have run out of Ethernet ports on my Modem. How do I add more computers?

Plugging in an Ethernet hub or switch expands the number of ports on the Modem. Run a standard Ethernet cable from the "Uplink" port of the new hub or switch to an Ethernet port on the Modem.

Which protocols does the Modem support?

The internal LAN connections support multiple protocols (e.g. TCP/IP, NetBEUI, IPX/SPX, and AppleTalk). The External WAN connection supports only TCP/IP.

Which connection speeds does the Modem support?

The LAN connections on the Modem support 10/100 Mbps. The WAN connection supports 8 Mbps, because of the physical restrictions placed on broadband connections. The 802.11g wireless connection supports up to 54 Mbps connection speeds (depending on signal quality, environmental factors, and physical distance).

Will my Xbox work with the Modem?

Yes, the Modem is compatible with the Xbox. You need to set a static IP on the Xbox in the Xbox live network settings, and forward ports 3074 (both UDP and TCP), 53 (both UDP and TCP), and 88 (UDP) if you run into DSL resolution errors.

Is the Modem flash-upgradeable? How do I do it?

Yes, the firmware is upgradeable. You can find a link to the firmware site under Utilitiesî in the Web-based configurator. We recommend contacting the ISP for assistance to avoid any issues running firmware upgrades, and to confirm you have the correct firmware before upgrading the unit.

Does the Modem function as a DSL modem?

Yes, the Modem has a built-in DSL Modem.

Wireless

Can I use an 802.11b wireless card to connect to the Modem?

Yes, the Modem can handle 802.11b cards or 802.11g cards. The 802.11g standard is backward compatible with the 802.11b standard. The Modem can be setup to handle just "g" wireless cards, just "b" wireless cards, or both.

If I install several Modems in different locations in my building, will they be able to talk to each other? Will I be able to stay connected as I move between them?

The Modem does not communicate with other access points, since it functions as a single access point system. If you installed several Modem devices and were to move between coverage areas, your wireless device would have to reconnect to a separate network.

Which wireless cards will work with the Modem?

The Modem connects with any wireless card supporting the 802.11g/802.11b wireless standards.

Can my wireless signal pass through floors, walls, and glass?

The physical environment surrounding the Modem can have a varying effect on signal strength and quality. Generally, the more dense the object (a concrete wall compared to a plaster wall, for example), the greater the interference. Concrete or metal-reinforced structures will experience a higher degree of signal loss than those made of wood, plaster, or glass.

I have an Apple computer that uses the Airport wireless device. Is this device compatible with the Modem?

While Apple Airport cards should work with the Modem, newer Apple systems may have patches installed that will not allow them to accept WEP keys. If you use new Apple Airport cards and have issues with WEP, set the Modem encryption to WPA (see "WPA" on page 18).

Network

I use my laptop at work and at home. Is there something special I need to do to make it work in both places?

Yes. Reconfigure your network setting (Workgroup, Domain, Password, User name, IP addressing or any other specific settings used by your company). You may also use third party software like NetSwitcher to automatically switch between different configurations.

What is the valid IP range I can use for my home network?

The valid IP range for the Modem is 192.168.0.2 to 192.168.0.254 by default.

How do I find out what IP address my computer is using?

Windows 2000 and XP - Select **Start**, **Run** and type "cmd." Press **Enter**. When the command screen appears, type "ipconfig" and press **Enter**.

I used DHCP to configure my network. Do I need to restart my computer to refresh my IP address?

No. Follow these steps to refresh your IP address:

Windows 2000 - Select **Start**, **Run**, type "cmd," and press **Enter**. At the DOS prompt, type "ipconfig /release," then type "ipconfig /renew."

Windows XP - Unplug the Ethernet cable or wireless card and plug it back in.

Can I run an application located on another computer over the network?

Yes, if the application is designed to run over a network.

Can I play games between computers on my network, or on the Internet?

Yes, if the games were designed for multi-player or LAN play. For specific information about whether a game is capable of Internet or LAN play, refer to the game documentation. Some games require ports to be forwarded to host or join games over the Internet.

I have an FTP or Web server on my network. How can I make it available to users on the Internet?

For a Web server, enable port forwarding for port 8088 to the IP address of the server and set up the Web server to receive on that port, as well. (Configuring the server to use a static IP address is recommended.)
For an FTP server, enable port forwarding for port 21 to the IP address of the server. (Configuring the server to use a static IP address is recommended.)

Connections

How many computers can be connected through the Modem?

The Modem is capable of 254 connections, but it is recommended to have no more than 45 connections. As you increase the number of connections, you decrease the available speed for each computer.

Security

What is the default username for the Modem?

The default username for the router is "admin" and the default password is "password" (all lower case, no quotation marks). To activate the password to protect the Modem, change the default password. Remote management will not be available on the Modem until the default password is changed.

Does the Modem function as a firewall?

Yes. The Modem provides its security through the use of NAT firewall, which acts as a physical barrier between your network and the Internet.

What is NAT and how does it protect my network?

NAT (Network Address Translation) is a type of security that masks the private IP addresses of the computers on your network with a single public IP address. With NAT, the private IP address of the computers on your network is never transmitted over the Internet.

Which Virtual Private Networking (VPN) protocols are supported?

The Modem supports pass-through for PPTP, L2TP, and IPSec.

This page left intentionally blank.

Specifications

A

General

Model Number

GT724WGR (Wireless DSL Modem)

Standards

IEEE 802.3 (10BaseT)
IEEE 802.3u (100BaseTX)
IEEE 802.11g (Wireless)
G.dmt
G.lite
t1.413
RFC 1483, 2364, 2516

Protocol

LAN - CSMA/CD
WAN - PPP, DHCP, Static IP

WAN

Full-rate ADSL Interface

LAN

10/100 RJ-45 switched ports

Speed

LAN Ethernet: 10/100 Mbps auto-sensing
Wireless: 802.11g 54 Mbps optimal (see "Wireless Operating Range" for details)

Cabling Type

Ethernet 10BaseT: UTP/STP Category 3 or 5
Ethernet100BaseTX: UTP/STP Category 5

Wireless Operating Range

Indoors

Up to 91M (300 ft.) @ 54 Mbps

Outdoors

Up to 457M (1500 ft.) @ 54Mbps

Topology

Star (Ethernet)

LED Indicators

Power, DSL, Internet, Ethernet (4), Wireless

Environmental

Power

External, 12V DC, 600mA

Certifications

FCC Class B, FCC Class C (part 15, 68), CE Mark Commercial, UL

Operating Temperature

0º C to 40º C (32ºF to 104ºF)

Storage Temperature

-20ºC to 70ºC (-4ºF to 158ºF)

Operating Humidity

10% to 85% non-condensing

Storage Humidity

5% to 90% non-condensing

Setting up Static IP on a Computer

B

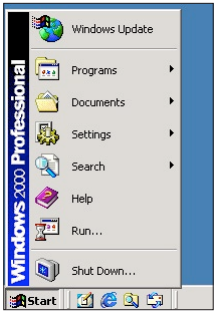
To communicate with the Modem from a computer on the network (to use the Modem's GUI, for example), the user may have to switch the IP address settings from DHCP-enabled to static IP on the computer, so that the computer and the Modem are on the same subnet.

To set up static IP on a computer, select the operating system and follow the instructions provided in this chapter.

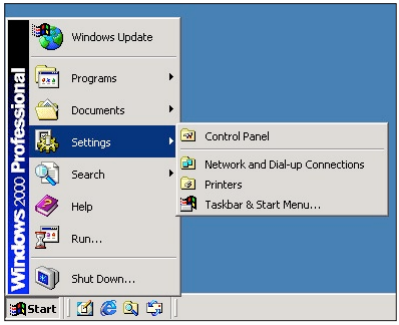
☞ ***Note***: The following insturctions are based on the Modem's factory default IP address. If the Modem's IP address has been changed, enter the new IP address when instructed to enter an IP address.

Windows 2000

1. From the desktop, click on the **Start** button in the lower left corner.
2. From the menu that appears, select **Settings**.

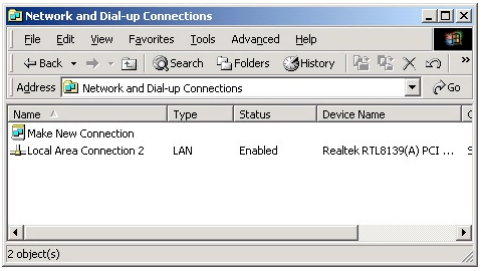


3. Another menu appears. Select **Control Panel**.

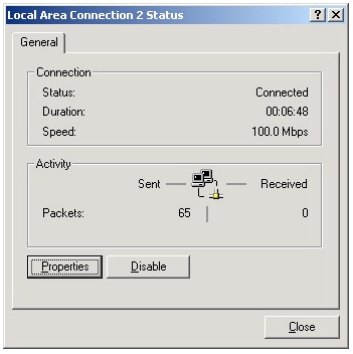


4. When the "Control Panel" window appears, double-click **Network and Dial-up Connections**.

5. In the "Network and Dial-up Connections" window, double-click **Local Area Connection**. A number may be displayed after the Local Area Connection. If there is more than one Local Area Connection listed, locate the one that corresponds to the network card installed in the computer by finding the name of the network card in the "Device Name" column.

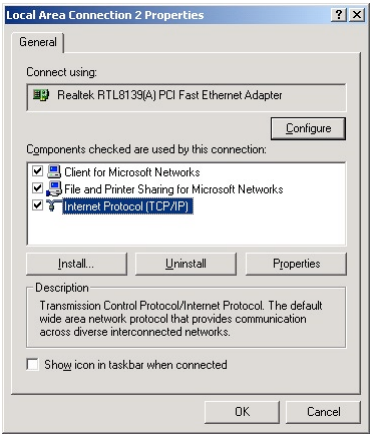

Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders History
Address Network and Dial-up Connections
Go
Name Type Status Device Name
Make New Connection
Local Area Connection 2 LAN Enabled Realtek RTL8139(A) PCI ...
2 object(s)

6. The "Local Area Connection Status" window appears. Select **General**, then click **Properties**.

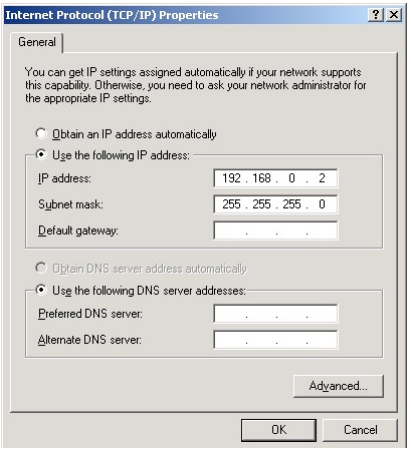


7. The "Local Area Connection Properties" window appears. Click **General**.

8. In the "Components checked are used by this connection" list box, double-click **Internet Protocol (TCP/IP)**.



9. The "Internet Protocol (TCP/IP) Properties" window appears.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 0 . 2
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

10. In the **General** tab, make sure the radio button next to "Obtain an IP Address automatically" is active (contains a black dot). If the radio button is already active, leave it alone.

11. Enter the following numbers in the "IP Address" text box:

192.168.0.2

Press the space bar on the keyboard to add the periods between the numbers.

12. Enter the following numbers in the "Subnet mask" text box:

255.255.255.0

Press the space bar on the keyboard to add the periods between the numbers.

13. Enter the following numbers in the "Default gateway" text box:

192.168.0.1

Press the space bar on the keyboard to add the periods between the numbers.

14. Click **OK**. The "Internet Protocol (TCP/IP) Properties" window disappears.

15 In the "Local Area Connection Properties" window, click **OK**. The Local Area Connection Properties window disappears.

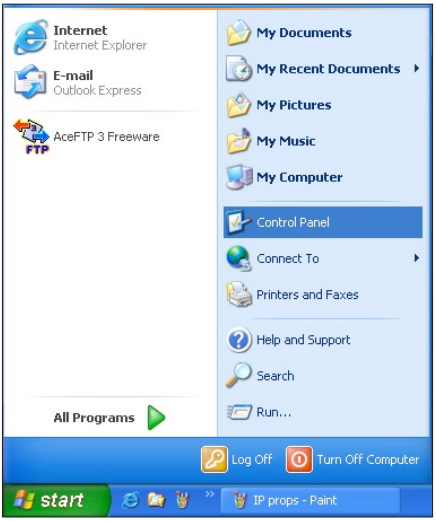
16. Click **Close** in the Local Area Connection Status window. The window disappears.

17. Close the Network and Dial-up Connections window by clicking on the "**x**" button at the upper right corner of the window.

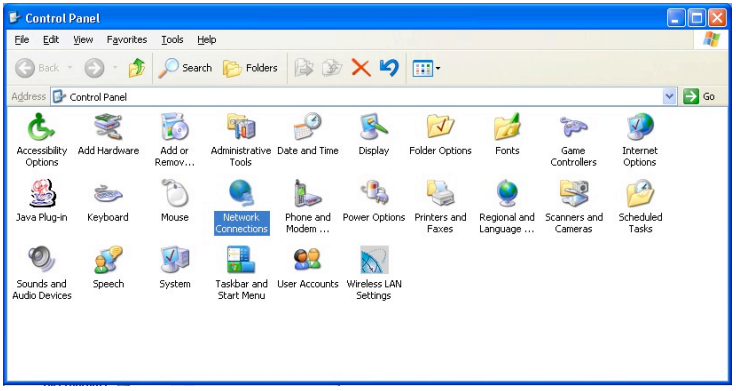
The computer is now set up with a static IP address, allowing the user to access the Modem's GUI.

Windows XP

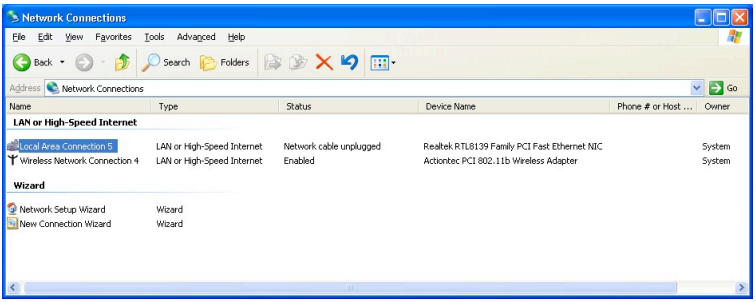
1. From the desktop, click **Start** button in the lower left corner.
2. From the menu that appears, select **Control Panel**.



3. When the "Control Panel" window appears, double-click **Network Connections**.

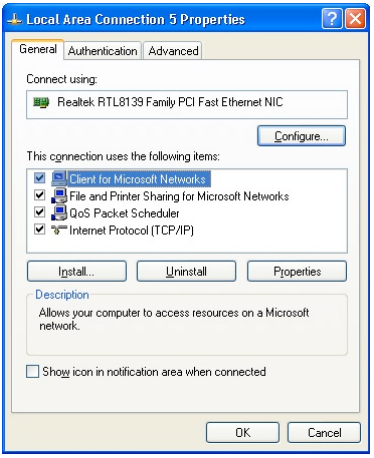


4. In the "Network Connections" window, double-click **Local Area Connection**. A number may be displayed after the Local Area Connection. If more than one Local Area Connection is listed, locate the one that corresponds to the network card installed in your computer by finding the name of the network card in the "Device Name" column.

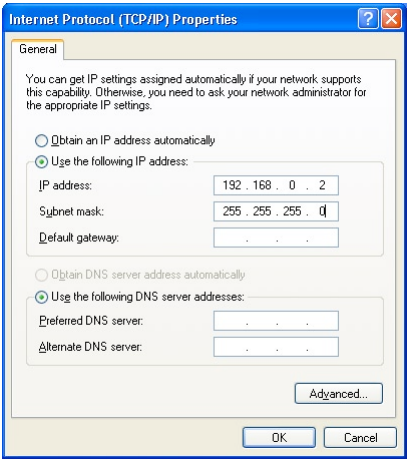

Network Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network Connections
Go
Name Type Status Device Name Phone # or Host ... Owner
LAN or High-Speed Internet
Local Area Connection 5 LAN or High-Speed Internet Network cable unplugged Realtek RTL8139 Family PCI Fast Ethernet NIC System
Wireless Network Connection 4 LAN or High-Speed Internet Enabled Actiontec PCI 802.11b Wireless Adapter System
Wizard
Network Setup Wizard Wizard
New Connection Wizard Wizard

5. The "Local Area Connection Properties" window appears. Select **General**.

6. In the "This connection uses the following items" list box, double-click **Internet Protocol (TCP/IP)**.


Local Area Connection 5 Properties
General Authentication Advanced
Connect using:
Realtek RTL8139 Family PCI Fast Ethernet NIC
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol (TCP/IP)
Install... Uninstall Properties
Description
Allows your computer to access resources on a Microsoft network.
Show icon in notification area when connected
OK Cancel

7. The "Internet Protocol (TCP/IP) Properties" window appears.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 0 . 2
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

8. In the **General** tab, make sure the radio button next to "Use the following IP Address" is active (contains a black dot). If the radio button is already active, leave it alone.

9. Enter the following address in the "IP Address" text box:

192.168.0.2

Enter the periods in the address by pressing the space bar on the keyboard.

10. Enter the following address in the "Subnet mask" text box:

255.255.255.0

Enter the periods in the address by pressing the space bar on the keyboard.

11. Enter the following address in the "Default gateway" text box:

192.168.0.1

Enter the periods in the address by pressing the space bar on the keyboard.

12. Click **OK**. The Internet Protocol (TCP/IP) Properties window disappears.

13 In the Local Area Connection Properties window, click **Close**. The Local Area Connection Properties window disappears.

14. Click **Close** in the Local Area Connection Status window. The window disappears.

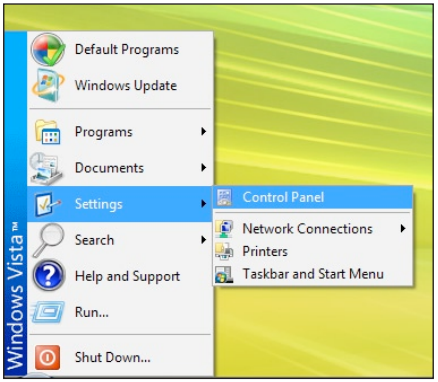
15. Close the Network and Dial-up Connections window by clicking on the "**x**" button at the upper right corner of the window.

The computer is now set up with a static IP address, allowing the user to access the Modem's GUI.

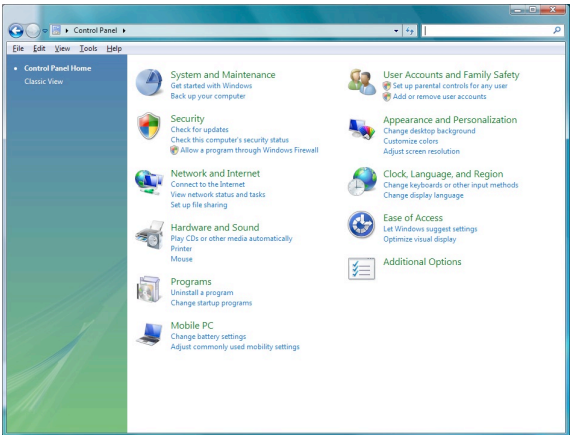
Windows Vista

1. From the desktop, click **Start** button in the lower left corner.

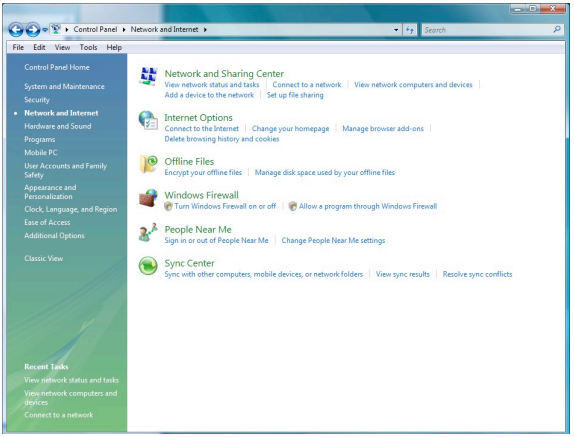
2. From the menu that appears, select **Control Panel**.



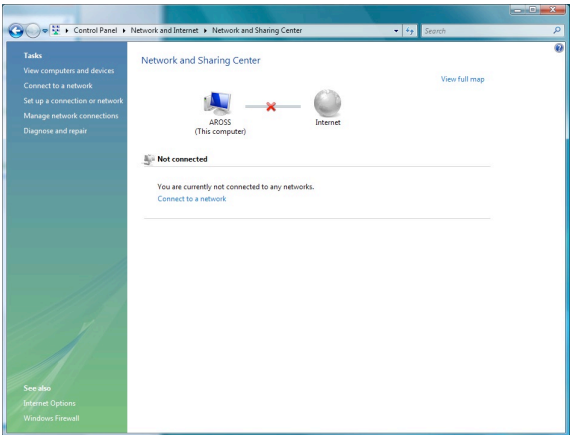
3. When the "Control Panel" window appears, double-click **Network and Internet**.



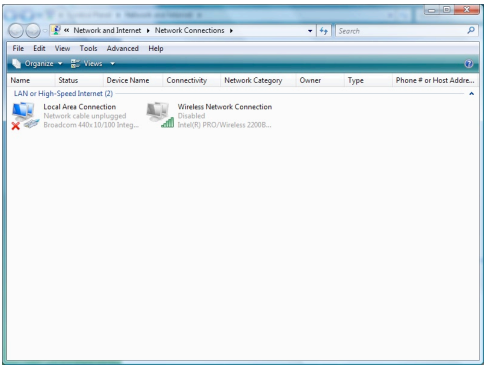
4. The "Network and Internet" window appears. Click **Network and Sharing Center**.


Control Panel ▸ Network and Internet ▸
Search
File Edit View Tools Help
Control Panel Home
System and Maintenance
Security
Network and Internet
Hardware and Sound
Programs
Mobile PC
User Accounts and Family Safety
Appearance and Personalization
Clock, Language, and Region
Ease of Access
Additional Options
Classic View
Network and Sharing Center
View network status and tasks | Connect to a network | View network computers and devices
Add a device to the network | Set up file sharing
Internet Options
Connect to the Internet | Change your homepage | Manage browser add-ons
Delete browsing history and cookies
Offline Files
Encrypt your offline files | Manage disk space used by your offline files
Windows Firewall
Turn Windows Firewall on or off | Allow a program through Windows Firewall
People Near Me
Sign in or out of People Near Me | Change People Near Me settings
Sync Center
Sync with other computers, mobile devices, or network folders | View sync results | Resolve sync conflicts
Recent Tasks
View network status and tasks
View network computers and devices
Connect to a network

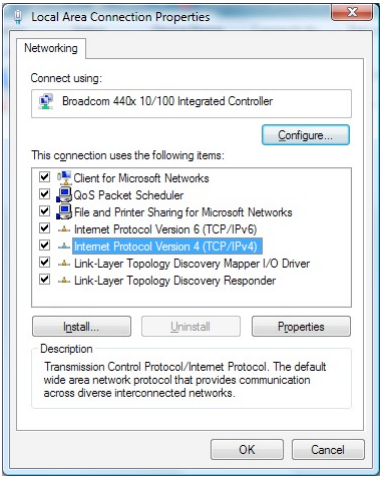
5. The "Network and Sharing Center" screen appears. From the menu on the left, click **Manage network connections**.



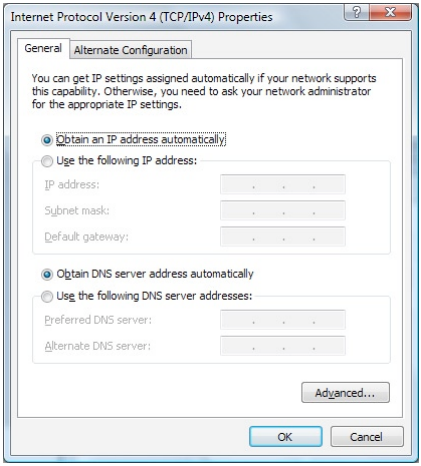
6. The "Network Connections" screen appears.. Double-click **Local Area Connection**.


Network and Internet ▸ Network Connections ▸
File Edit View Tools Advanced Help
Organize Views
Name Status Device Name Connectivity Network Category Owner Type Phone # or Host Addre...
LAN or High-Speed Internet (2)
Local Area Connection
Network cable unplugged
Broadcom 440x 10/100 Integ...
Wireless Network Connection
Disabled
Intel(R) PRO/Wireless 2200B...

7. The "Local Area Connection Properties" window appears. In the "This connection uses the following items" list box, double-click **Internet Protocol (TCP/IP)**.



8. The "Internet Protocol (TCP/IP) Properties" window appears.


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

9. In the **General** tab, make sure the circle next to "Use the following IP Address" is selected. When active, a black dot appears in the circle. If the circle already contains a black dot, leave it alone.

10. Enter the following address in the "IP Address" text box:

192.168.0.2

Enter the periods in the address by pressing the space bar on the keyboard.

11. Enter the following address in the "Subnet mask" text box:

255.255.255.0

Enter the periods in the address by pressing the space bar on the keyboard.

12. Enter the following address in the "Default gateway" text box:

192.168.0.1

Enter the periods in the address by pressing the space bar on the keyboard.

13. Click **OK**. The Internet Protocol (TCP/IP) Properties window disappears.

14. In the Local Area Connection Properties window, click **Close**. The Local Area Connection Properties window disappears.

15. Click **Close** in the Local Area Connection Status window. The window disappears.

16. Close the rest of the open windows by clicking on the "**x**" button at the upper right corner of the window.

The computer is now set up with a static IP address.

Service Acronyms

C

The following information is related to the Firewall options (Custom, High, Medium, and Low) section in the "Configuring Security Settings" chapter of this manual. This appendix explains the meaning of the service acronyms included with the various levels of firewall security, and the UDP and TCP ports used by each service.

Service Acronym Definitions

DNS

Domain **N**ame **S**ystem. A data query system used to translate host names into Internet addresses (i.e., www.somewebsite.com translates to 888.999.000.111). Uses UDP 53 and TCP 53.

EPMAP

End**P**oint **Map**per. Uses UDP 135 and TCP 135.

FTP

File **T**ransfer **P**rotocol. A protocol used to transfer files over the Internet. Uses TCP 20 and 21.

HTTP

Hyper**T**ext **T**ransfer **P**rotocol. This protocol delivers information over the Internet, and is used when a computer connects to a Web site via an Internet browser. Uses TCP 80.

HTTPS

Hyper**T**ext **T**ransfer **P**rotocol using **S**ecure Socket Layer. A secure version of the protocol that delivers information over the Internet. Uses UDP 443 and TCP 443.

IMAP, IMAPv3

Internet **M**essage **A**ccess **P**rotocol. Protocols for retrieving E-mail messages. IMAP uses TCP 143; IMAPv3 uses TCP 220.

IPSEC IKE, IPSEC ESP

IP Security. Protocols which support the secure exchange of packets at the IP layer**.** Uses UDP 500.

LDAP

Lightweight **D**irectory **A**ccess **P**rotocol. A set of protocols for accessing information directories. Uses TCP 389.

MICROSOFT-DS, -GC

-DS uses UDP 445 and TCP 445; -GC uses TCP 3268.

NETBIOS-NS, -DGM, -SSN

Network **B**asic **I**nput **O**utput **S**ystem. Three types of DOS BIOS augmentation which add functions for local area networks (LANs). -NS uses UDP 137 and TCP 137; -DGM uses UDP 138; -SSN uses TCP 138.

NNTP

Network **N**ews **T**ransfer **P**rotocol. A protocol used to distribute and retrieve news articles over the Internet. Uses TCP 119.

POP3

Post **O**ffice **P**rotocol 3. Another protocol used to transfer E-mail between computers. Usually employs a pop3 server, and is used to receive mail only. Uses TCP 110.

PROFILE

Uses TCP 136.

SMTP

Simple **M**ail **T**ransfer **P**rotocol. A protocol used to transfer E-mail between computers over the Internet. Can be used to send and receive mail. Uses TCP 25.

SNMP

Simple **N**etwork **M**anagement **P**rotocol. A set of protocols for managing networks. Uses UDP 161.

This page left intentionally blank.

Glossary

D

Access Point

A device that allows wireless clients to connect to one another. An access point can also act as a bridge between wireless clients and a "wired" network, such as an Ethernet network. Wireless clients can be moved anywhere within the coverage area of the access point and remain connected to the network. If connected to an Ethernet network, the access point monitors Ethernet traffic and forwards appropriate Ethernet messages to the wireless network, while also monitoring wireless traffic and forwarding wireless client messages to the Ethernet network.

ATM (Asynchronous Transfer Mode)

A networking technology based on transferring data in fixed-size packets

Client

A desktop or mobile computer connected to a network.

DHCP (Dynamic Host Configuration Protocol)

A protocol designed to automatically assign an IP address to every computer on your network.

DNS (Domain Name System) Server Address

Allows Internet host computers to have a domain name and one or more IP addresses. A DNS server keeps a database of host computers and their respective domain names and IP addresses so that when a user enters a domain name into a Web browser, the user is sent to the proper IP address. The DNS server address used by computers on the home network corresponds to the location of the DNS server the ISP has assigned.

DSL (Digital Subscriber Line) Modem

A modem that uses existing phone lines to transmit data at high speeds.

Encryption

A method to allow wireless data transmissions a level of security.

ESSID (Extended Service Set Identifier)

A unique identifier for a wireless network. Also known as "SSID."

Ethernet Network

A standard wired networking configuration using cables and hubs.

Firewall

A method preventing users outside the network from accessing and/or damaging files or computers on the network.

Gateway

A central device that manages the data traffic of your network, as well as data traffic to and from the Internet.

IP (Internet Protocol) Address

A series of four numbers separated by periods identifying a unique Internet computer host.

ISP Gateway Address

An IP address for the Internet router. This address is only required when using a cable or DSL modem.

ISP (Internet Service Provider)

A business that allows individuals or businesses to connect to the Internet.

LAN (Local Area Network)

A group of computers and devices connected together in a relatively small area (such as a house or an office). A home network is considered a LAN.

MAC (Media Access Control) Address

The hardware address of a device connected to a network.

NAT (Network Address Translation)

A method allowing all of the computers on a home network to use one IP address, enabling access to the Internet from any computer on the home network without having to purchase more IP addresses from the ISP.

PC Card

An adapter that inserts in the PCMCIA slot of a computer, enabling the communication with a device.

PPPoE (Point-To-Point Protocol over Ethernet)/
PPPoA (Point-To-Point Protocol over ATM)

Methods of secure data transmission.

Router

A central device that manages the data traffic of your network.

Subnet Mask

A set of four numbers configured like an IP address used to create IP address numbers used only within a particular network.

SSID

See "ESSID."

TCP/IP (Transmission Control Protocol/Internet Protocol)

The standard protocol for data transmission over the Internet.

WAN (Wide Area Network)

A network that connects computers located in separate areas, (i.e., different buildings, cities, countries). The Internet is a WAN.

WECA (Wireless Ethernet Compatibility Alliance)

An industry group that certifies cross-vender interoperability and compatibility of IEEE 802.11b wireless networking products and promotes the standard for enterprise, small business, and home environments.

WLAN (Wireless Local Area Network)

A group of computers and other devices connected wirelessly in a small area.

This page left intentionally blank.

Notices

Regulatory Compliance Notices

Class B Equipment

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by implementing one or more of the following measures:

- Reorient or relocate the receiving antenna;
- Increase the separation between the equipment and receiver;
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected;
- Consult the dealer or an experienced radio or television technician for help.

Modifications

The FCC requires the user to be notified that any changes or modifications made to this device that are not expressly approved by A*ction*tec Electronics, Inc., may void the user's authority to operate the equipment.

Declaration of conformity for products marked with the FCC logo – United States only.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference;

2. This device must accept any interference received, including interference that may cause unwanted operation.

☞ ***Note***: To comply with FCC RF exposure compliance requirements, the antenna used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

For questions regarding your product or the FCC declaration, contact:

*Action*tec Electronics, Inc.
760 North Mary Ave.
Sunnyvale, CA 94086
United States
Tel: (408) 752-7700
Fax: (408) 541-9005

Limited Warranty

Hardware: *Action*tec Electronics, Inc., warrants to the end user ("Customer") that this hardware product will be free from defects in workmanship and materials, under normal use and service, for twelve (12) months from the date of purchase from *Action*tec Electronics or its authorized reseller.

*Action*tec Electronics' sole obligation under this express warranty shall be, at *Action*tec's option and expense, to repair the defective product or part, deliver to Customer an equivalent product or part to replace the defective item, or if neither of the two foregoing options is reasonably available, *Action*tec Electronics may, in its sole discretion, refund to Customer the purchase price paid for the defective product. All products that are replaced will become the property of *Action*tec Electronics, Inc. Replacement products may be new or reconditioned. *Action*tec Electronics warrants any replaced or repaired product or part for ninety (90) days from shipment, or the remainder of the initial warranty period, whichever is longer.

Software: *Action*tec Electronics warrants to Customer that each software program licensed from it will perform in substantial conformance to its program specifications, for a period of ninety (90) days from the date of purchase from *Action*tec Electronics or its authorized reseller. *Action*tec Electronics warrants the media containing software against failure during the warranty period. The only updates that will be provided are at the sole discretion of *Action*tec Electronics and will only be available for download at the *Action*tec Web site, www.actiontec.com. *Action*tec Electronics' sole obligation under this express warranty shall be, at *Action*tec Electronics' option and expense, to refund the purchase price paid by Customer for any defective software product, or to replace any defective media with software which substantially conforms to applicable *Action*tec Electronics published specifications. Customer assumes responsibility for the selection of the appropriate applications program and associated reference materials. *Action*tec Electronics makes no warranty or representation that its software products will meet Customer's requirements or work in combination with any hardware or applications software products provided by third parties, that the operation of the software products will be uninterrupted or error free, or that all defects in the software products will be corrected. For any third-party products listed in the *Action*tec Electronics software product documentation or specifications as being compatible, *Action*tec Electronics will make reasonable efforts to provide compatibility, except where the non-compatibility is caused by a "bug" or defect in the third party's product or from use of the software product not in accordance with *Action*tec Electronics published specifications or user guide.

THIS *ACTION*TEC ELECTRONICS PRODUCT MAY INCLUDE OR BE BUNDLED WITH THIRD-PARTY SOFTWARE, THE USE OF WHICH IS GOVERNED BY A SEPARATE END-USER LICENSE AGREEMENT.

THIS *ACTION*TEC ELECTRONICS WARRANTY DOES NOT APPLY TO SUCH THIRD-PARTY SOFTWARE. FOR THE APPLICABLE WARRANTY, PLEASE REFER TO THE END-USER LICENSE AGREEMENT GOVERNING THE USE OF SUCH SOFTWARE.

Obtaining Warranty Service: Customer may contact *Action*tec Electronics Technical Support Center within the applicable warranty period to obtain warranty service authorization. Dated proof of purchase from *Action*tec Electronics or its authorized reseller may be required. Products returned to *Action*tec Electronics must be pre-authorized by *Action*tec Electronics with a Return Merchandise Authorization (RMA) number marked on the outside of the package, and sent prepaid and packaged appropriately for safe shipment, and it is recommended that they be insured or sent by a method that provides for tracking of the package. The repaired or replaced item will be shipped to Customer, at *Action*tec Electronics' expense, not later than thirty (30) days after *Action*tec Electronics receives the defective product.

Return the product to:
(In the United States)
*Action*tec Electronics, Inc.
760 North Mary Avenue
Sunnyvale, CA 94085

*Action*tec Electronics shall not be responsible for any software, firmware, information, memory data, or Customer data contained in, stored on, or integrated with any products returned to *Action*tec Electronics for repair, whether under warranty or not.

WARRANTIES EXCLUSIVE: IF AN *ACTION*TEC ELECTRONICS' PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY FOR BREACH OF THAT WARRANTY SHALL BE REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT *ACTION*TEC ELECTRONICS' OPTION. TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, TERMS OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, AND NON-INFRINGEMENT, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. *ACTION*TEC ELECTRONICS

NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

*ACTION*TEC ELECTRONICS SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT OR MALFUNCTION IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPT TO OPEN, REPAIR OR MODIFY THE PRODUCT, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OTHER HAZARDS, OR ACTS OF GOD.

LIMITATION OF LIABILITY: TO THE FULL EXTENT ALLOWED BY LAW, *ACTION*TEC ELECTRONICS ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCT, EVEN IF *ACTION*TEC ELECTRONICS OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT,OR REFUND OF THE PURCHASE PRICE PAID, AT *ACTION*TEC ELECTRONICS' OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

Disclaimer: Some countries, states or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers, or the limitation of liability for personal injury, so the above limitations and exclusions may be limited in their application to you. When the implied warranties are not allowed to be excluded in their entirety, they will be limited to the duration of the applicable written warranty. This warranty gives you specific legal rights which may vary depending on local law.

Dispute Resolution: The customer may contact the Director of Technical Support in the event the Customer is not satisfied with *Action*tec Electronics' response to the complaint. In the event that the Customer is still not satisfied with the response of the Director of Technical Support, the Customer is instructed to contact the Director of Marketing. In the event that the Customer is still not satisfied with the response of the Director of Marketing, the Customer is instructed to contact the Chief Financial Officer and/or President.

Governing Law: This Limited Warranty shall be governed by the laws of the State of California, U.S.A., excluding its conflicts of laws and principles, and excluding the United Nations Convention on Contracts for the International Sale of Goods.